Computação

Rede de Computadores

Marcial Porto Fernández

Fortaleza

2019

Sumário

Apresentação

Desde o momento em que os sistemas de computadores deixaram de ter uma entidade central única - mas um conjunto de computadores trabalhando simultaneamente, as redes de computadores tornaram-se importantes. Com o crescimento do uso de computadores pessoais e a criação da Internet, surgiu uma nova arquitetura de processamento e difusão de informação universal que mudou o mundo.

Além disso, a velocidade de sua adoção foi a maior já registrada na história. Vale lembrar que enquanto a eletricidade levou mais de 100 anos desde a sua descoberta até ser usada pelas pessoas, as redes de computadores se tornaram amplamente utilizadas em pouco mais de 10 anos após sua criação.

Já no início do Século XXI foi possível considerar que o acesso à Internet se tornou uma necessidade básica do ser humano, assim como água, esgoto e energia elétrica. Alguns países já consideram a Internet como direito fundamental dos seus cidadãos, assim como escola e saúde. A Internet provoca impacto em todas as áreas da vida, desde a prestação de serviços bancários, comércio além de estabelecer comunicação entre as pessoas não importando a distância.

Este livro apresenta uma introdução às redes de computadores desde os seus princípios básicos até as aplicações mais conhecidas. O texto é dividido em três partes. A primeira trata de fundamentos da comunicação de dados e os fatores físicos de uma comunicação. A segunda parte apresenta conceitos de um protocolo de comunicações mostrando os mecanismos para estabelecer uma comunicação. A terceira parte mostra os principais protocolos que compõe a Internet e mostra como eles funcionam.

O Autor

Capítulo 1

Fundamentos de Redes de Computadores

Objetivos

- Nesta unidade vamos apresentar os conceitos básicos de Redes de Computadores. Iniciamos com a definição de alguns conceitos que serão necessários para o entendimento de uma rede de computadores. Depois apresentamos os princípios da transmissão de dados e a codificação de dados. Finalmente apresentamos algumas interfaces de comunicação de dados.

1. Introdução à Comunicação de Dados

Século XX é marcado pelo desenvolvimento das tecnologia e uso da informação. Cada vez mais a informação e sua difusão passa a ter um valor importante para as sociedades modernas. Os computadores inicialmente eram centralizados e a informação tinha um alcance limitado, geralmente à sala do CPD. Na década de 70 o uso de computadores autônomos cresceu com o desenvolvimento dos microprocessadores. O aumento de computadores autônomos propiciou o desenvolvimento de tecnologias que permitissem que esses sistemas se comunicar e trocar informações. Nas décadas de 80 e 90 essas tecnologias cresceram em velocidade e importância.

O objetivo desse capítulo é apresentar uma introdução histórica da comunicação de dados e alguns conceitos básicos de formalização. A Seção 1.1 apresenta um resumo da história da Internet e sua importância para vida atual. A Seção 1.2 mostra o modelo de comunicação de dados e a Seção 1.5 define conceitualmente um protocolo de comunicação. Finalmente, a Seção 1.6 apresenta as instituições de normatização da infraestrutura de comunicação.

1.1 História da Internet

Em meados dos anos 60, em plena Guerra Fria, o DoD (Departamento de Defesa dos Estados Unidos) precisou desenvolver um sistema de comunicações que sobrevivesse a uma guerra nuclear. O sistema telefônico tradicional é vulnerável, pois o rompimento de um cabo ou uma estação de trânsito interrompe todas as comunicações que passam por ele.

A ARPA (Agência de Pesquisa Militar dos Estados Unidos) avaliou que a solução era implementar uma rede de comutação de pacotes, que permitiria a comunicação entre terminais de mainframe. Nesta rede o importante é o endereço do destino e não o caminho que ele deve fazer, assim, se um cabo ou comutador fosse destruído, as comunicações continuariam fluindo por outro caminho. Foi criada então a ARPANET (Figura 1.1.1), rede que interligava as Forças Armadas, Governo, Universidades (que desenvolviam o projeto) e empresas fabricantes de materiais bélicos.

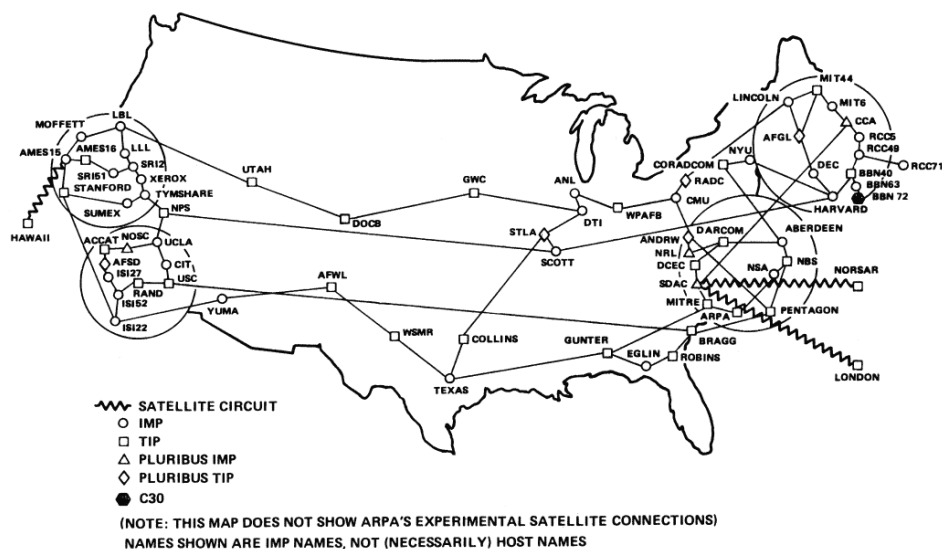



Figura 1.1.1: Arpanet em outubro de 1980

Com o crescimento da ARPANET, observou-se que o protocolo não era adequado para funcionar com uma quantidade grande de subredes. Assim foi desenvolvido na Universidade de Berkeley (1974) o protocolo TCP/IP. Esse protocolo foi adicionado ao sistema Unix já desenvolvido nesta universidade no qual foi chamado de BSD versão 4.2.

O sistema operacional Unix BSD já era usado em várias universidades do mundo e a atualização desta versão introduziu o protocolo TCP/IP e a interface Socket no meio acadêmico. Esse aumento de novos equipamentos conectados fez, em 1983, que a ARPANET se dividisse em duas redes, uma apenas militar que foi chamada MILNET, e a ARPANET que continuou sendo usada pelas universidades.

No final dos anos 80 a rede ARPANET passou a se chamar INTERNET. Ao longo dos anos, muitas aplicações foram sendo criadas, como Telnet, E-mail, FTP, etc, mas a grande revolução foi em 1990, quando cientistas do CERN (Laboratório de Física na Suíça) criaram o WWW (World Wide Web).

O WWW oferece uma interface gráfica, muito mais amigável que a interface texto. A possibilidade de usar várias mídias juntas como texto, imagens, som, vídeo e a característica de se transferir para outra página, em qualquer lugar do mundo, com apenas um clic do mouse, tornou a Internet acessível por qualquer pessoa, mesmo as que não tinham nenhum conhecimento de informática.

A Internet contabilizava mais de 15 milhões de usuários no início de 1996 e estima-se ter chegado a 1,6 bilhões de usuários em 2010. O tráfego

total estimado chega a 1 ZettaByte (1021) em 2010. Inicialmente a Internet foi uma ferramenta importante para o meio acadêmico mas hoje é essencial para as empresas e, cada vez mais, para o uso pessoal.

Esse grande número de usuários tornou necessárias mudanças no endereçamento IP, pois a capacidade de endereçamento do protocolo atual estará esgotado em poucos tempo. Além disso, o uso de dados multimídia, tem exigido do protocolo garantias de qualidade quanto tempo de chegada dos pacotes no destino. Outro problema é a questão de segurança, pois como a rede foi concebida no meio acadêmico, não era necessário esconder qualquer dado. Hoje com o uso comercial da rede é necessário segurança para poder ser efetuadas compras e transações financeiras. Todos esses problemas serão resolvidos com a introdução do novo protocolo IPv6, ainda pouco usado mas que se tornará padrão em alguns anos.

1.2 Modelo de Comunicação

Mostramos na Figura 1.1.2 o modelo genérico de uma comunicação. A máquina cliente solicita uma requisição (request) a máquina servidora, que entende a requisição e devolve para o cliente a resposta solicitada (reply).

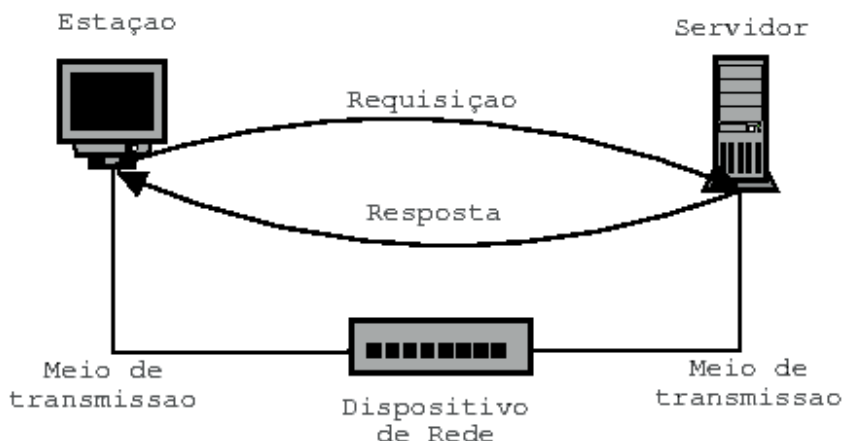



Figura 1.1.2: Modelo de uma comunicação

Servidores e clientes são computadores com um sistema operacional conectados em rede. Essa comunicação deve ser a mais transparente possível para permitir que um maior número de usuários com sistemas operacionais diferentes possam requisitar informações dos servidores. Por isso a comunicação, isto é, seus protocolos de redes, devem ser padronizados.

1.2.1 Cliente

Um cliente é um equipamento que estabelece a interface do usuário com a rede. Uma estação pode ser um computador pessoal, notebook, PDA ou tele-

fone celular. Em uma arquitetura cliente-servidor, o cliente é responsável pela exibição das informações para o usuário de forma amigável, por exemplo, interface gráfica, e realiza um condicionamento dos dados que serão transmitidos para o servidor, por exemplo, criptografando os dados sensíveis antes de transmitir pela rede.

Para o usuário a utilização de uma aplicação no cliente é transparente pois ele é responsável pela transmissão e recepção dos dados com o servidor. O programa cliente é responsável por estabelecer, manter e encerrar a comunicação assim como detectar e corrigir os erros de transmissão e dosar a taxa de transmissão de acordo com a capacidade da rede.

1.2.2 Servidor

Servidor é o equipamento que fornece informações mediante solicitação de um cliente. Geralmente é um computador com maior capacidade pois processa o serviço de comunicação para vários clientes além de gerenciar bancos de dados que contém as informações.

Como os servidores geralmente são únicos, é necessário fornecer uma infraestrutura confiável. Para isso, discos redundantes e fontes de alimentação ininterrupta (no-break) são equipamentos úteis.

1.2.3 Meio de transmissão

Meio de transmissão é o meio físico por onde os dados vão trafegar entre cliente e servidor. Vários meios físicos podem ser utilizados, cada um de acordo com o ambiente e a distância desejada. Alguns exemplos podem ser: par trançado, cabo coaxial, fibra ótica ou rádio (sem fio).

1.2.4 Dispositivos de rede

Se cliente e servidor estão distantes, é necessário recuperar o sinal de transmissão ao longo do caminho. Se a ligação é compartilhada com outros cliente e servidores, é necessário interligar todos os dispositivos e encaminhar corretamente todas as mensagens. Os dispositivos podem ser repetidores, hubs, comutadores (switchs) ou roteadores.

1.3 Redes de comunicação de dados

A comunicação de dados entre dois dispositivos tem aplicação limitada. Quando estabelecemos comunicação entre mais de dois dispositivos construímos uma rede de comunicação de dados.

As redes de comunicação de dados podem ser classificadas confor-

me a distância de alcance que envolve tecnologias e mecanismos diferentes. Apresentamos, a seguir, a classificação de redes conforme a distância e um sumário dos diversos dispositivos de rede existentes.

1.3.1 LAN

Local Area Network - Rede local. Rede de computadores de âmbito local com distâncias da ordem de centenas de metros e utilizando protocolos LAN como Ethernet, Token-Ring ou FDDI

A LAN ou rede local é uma rede que conecta dispositivos próximos, com distâncias da ordem de dezenas a centenas de metros, tipicamente instaladas em prédios. Pelo fato da proximidade e por sofrer menos interferência (ruídos) do meio ambiente, existe possibilidade o uso de tecnologias distintas das redes WAN, redes de longa distância.

Uma LAN apresenta velocidades significativamente maiores do que nas redes WAN aproveitando a menores distâncias. Como uma LAN está sob controle de uma única organização não há preocupação em bilhetagem ou controle do uso pois todos os usuários pertencem à organização e os equipamentos geralmente pertencem à ela.

Normalmente uma LAN apresenta um funcionamento baseado na difusão de dados (broadcast) contra o funcionamento comutado de uma rede WAN. Como o meio tem alta capacidade e os dispositivos pertencem à organização, esse modo de funcionamento é bastante eficiente e barato.

1.3.2 WAN

Wide Area Network - Rede que interliga computadores distribuídos em áreas geograficamente distantes.

Uma rede WAN ou rede de longa distância conecta dispositivos com distâncias grandes, d a ordem de dezenas ou centenas de quilometros. Pelo fato das grandes distâncias a velocidade é geralmente menor do que alcançadas nas redes locais LAN, pois nesse caso as interferências e ruídos são fatores limitantes. Os equipamentos são mais sofisticados e complexos, apresentando custos maiores.

1.3.3 MAN

Metropolitan Area Network - Rede que interliga computadores distribuídos em uma área metropolitana, tipicamente no âmbito de uma cidade.

A MAN é uma rede de âmbito metropolitano, com distâncias até dezenas de quilômetros. Como nessa distância as tecnologias de redes LAN

não podem ser utilizadas torna-se necessário o uso de tecnologias de longa distância WAN. Por esse fato, a nomenclatura MAN tem sido substituída pela nomenclatura WAN pois são as tecnologias utilizadas nessas distâncias.

1.3.4 Dispositivos de rede

Os equipamentos de conectividade são todos os dispositivos que estabelecem a comunicação entre dois pontos. Eles são responsáveis por recuperar o sinal, detectar e corrigir erros de transmissão e encaminhar as mensagens para o destino correto. Apresentaremos a seguir um breve resumo de suas características de cada um.

Placa de rede

A placa de rede, também chamada NIC, é um acessório que possibilita um computador a se ligar em rede. Existem vários protocolos de rede e forma de conexão ao computador, possibilitando diferentes padrões e velocidades.

Repetidor

Dispositivo de rede de camada 1 do modelo OSI responsável por repetir as mensagens entre duas portas, pertencentes ao mesmo segmento de rede.

Os repetidores são equipamentos que permitem aumentar a distância entre dois dispositivos em uma rede local (LAN). O repetidor atua na camada Física do modelo OSI e consiste basicamente em amplificar e regenerar os sinais recebidos em uma porta para outra.

Hub

Repetidor com múltiplas portas. Dispositivo de rede de camada 1 do modelo OSI responsável por repetir as mensagens em todas as portas, pertencentes ao mesmo segmento de rede.

Um hub é um repetidor com múltiplas portas. Um sinal recebido em uma porta é repetido para todas as demais portas. Tipicamente o hub é o elemento central de uma topologia estrela. Assim como o repetidor, o hub atua na camada física do modelo OSI e pode dispor de portas de mídias diferentes (par trançado, coaxial e fibra ótica) porém a velocidade e os protocolos de enlace devem ser idênticos.

Bridge (ponte)

Dispositivo de rede de camada 2 do modelo OSI responsável por filtrar a passagem de mensagens entre dois segmentos de rede.

Uma bridge é um dispositivo que isola segmentos de redes locais. Ela manipula mensagens ao invés de repetir o sinal elétrico, como no caso do repetidor, por isso é um dispositivo da camada 2 do modelo OSI (Enlace).

Uma bridge dispõe de duas portas e suas funções são: filtrar as mensagens de acordo com o endereço de destino, repetindo para outra porta apenas as mensagens referentes a este segmento de rede e armazenar as mensagens se o segmento de destino estiver ocupado. Outra função é verificar o estado das mensagens e descartar se ela contém algum erro, possibilitando assim que uma mensagem com erro não precise viajar até o destinatário para ter o erro identificado.

Como atua na camada 2 uma bridge pode interligar redes com velocidades diferentes, por exemplo, Ethernet 10 MBPS e Fast-Ethernet 100 MBPS.

Switch (Comutador)

Dispositivo de rede de camada 2 do modelo OSI responsável por encaminhar mensagens para o segmento onde está o destinatário. Ele transmite mensagem apenas para dispositivos diretamente conectador.

Um switch é uma bridge com várias portas para interligar vários segmentos de rede. A função do swich é encaminhar a mensagem apenas para o segmento onde o destinatário se encontra.

Ao ligar um switch ele inicia o modo de aprendizado, colocando o endereço de origem de cada mensagem recebida em cada porta. Ao receber uma mensagem para este endereço de destino ele envia para a porta associada. Se o endereço de destino não for encontrado na tabela é realizado uma difusão (broadcast) em todas as portas do dispositivo para identificar a porta a ser utilizada.

Como os switchs são dispositivos simples que requerem altas velocidades ele geralmente é implementado somente com hardware.

Roteador (Router)

Dispositivo de rede de camada 3 do modelo OSI (Rede) responsável por encaminhar mensagens para o destinatário mesmo que ele não esteja conectado diretamente, tomando como referência uma tabela de rotas.

Enquanto um switch mantém uma tabela de endereços apenas dos equipamentos ligados em cada segmento de rede, o roteador é responsável por encaminhar as mensagens para o caminho certo, mesmo que o destinatário não se encontre nos segmentos de rede diretamente ligados a ele. Por isso um roteador é um dispositivo da camada 3 do modelo OSI.

Para decidir a rota, o roteador consulta uma tabela de roteamento que contém a informação de todos os destinos alcançáveis. Essas tabelas podem

ser estáticas, configuradas pelo operador da rede, ou dinâmica, através dos protocolos RIP ou OSPF. Por essa razão os roteadores requerem maior poder computacional (CPU e memória) que os switchs, além de serem implementados basicamente em software.

Roteadores podem interligar protocolos e velocidades diferentes, como ligação de uma rede local (LAN) na velocidade da ordem de MBPS, com redes de longa distância (WAN) na velocidade da ordem de KBPS. Pela sua abrangência o roteador pode ser utilizado em redes locais, redes de longa distância e nos núcleos das redes dos operadores de telecomunicações.

Servidor de Terminais (Terminal Server)

O servidor de terminais é um dispositivo que possibilita a ligação de uma rede local com dispositivos de baixa velocidade via interface serial (RS-232) como terminais, impressoras, balanças, caixa registradores e modems.

Servidor de Acesso Remoto (RAS)

Equipamento de rede utilizado para estabelecer a interligação de dispositivos remotos (por exemplo, computadores com modem) com uma rede privada.

O RAS é um Servidor de Terminais mais sofisticado usado principalmente na interligação de uma rede local com a rede de telefonia pública. Como ele está ligado a uma rede pública é necessário dispor de funções de autenticação, verificação e contabilidade. Além disso ele pode se ligar a rede pública através de canais digitais E1 que possibilita um maior velocidade de acesso e facilitam o cabeamento.

Gateway

Um gateway atua em todas as camadas do modelo OSI e tem como objetivo permitir a comunicação entre redes com arquiteturas distintas. Alguns dos problemas dessa integração são tamanho máximo de pacotes, formas de endereçamento, técnicas de roteamento, controle de acesso, temporizações, etc. Um exemplo de gateway é interligação de redes TCP/IP com redes SNA, permitindo o acesso de mainframe através de emulação de terminal.

1.4 Modelo de Referência

1.4.1 Modelo de Referência OSI

Em 1983 a ISO, definiu um modelo de comunicação para sistemas abertos OSI. Esse modelo foi dividido em sete camadas executando funções do meio físico até a aplicação, mostrado na Figura 1.1.3.

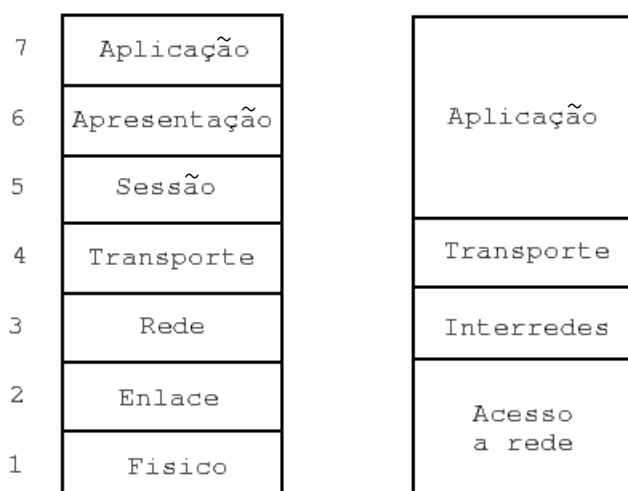



Figura 1.1.3: Modelo OSI e Internet.

SAP Service Access Point (ponto de acesso ao serviço). Ponto de comunicação entre duas camadas de um protocolo

Cada camada é responsável por uma determinada função e entre elas existe um ponto de acesso comum chamado SAP. A ideia é que cada camada possa ser trocada por outra de padrão diferente mas com a mesma função. Cada camada é apresentada a seguir na Figura 1.1.4.

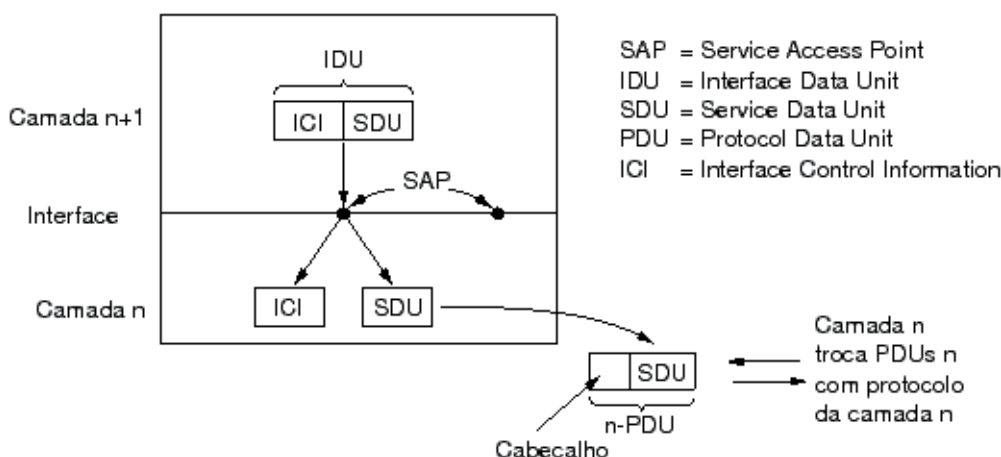



Figura 1.1.4: Relacionamento entre duas camadas de protocolo.

Camada Física

É a interface com o meio de comunicação e está voltada para as funções mais básicas. Os problemas tratados nesta camada são os mais próximos do hardware como tensão do bit “1” frequência do sinal, etc.

Camada de Enlace de Dados

É responsável por tratar os dados brutos da camada inferior e oferecer a camada superior dados livres de erros de transmissão. Ela é responsável pelo controle de erro, envio de reconhecimento e corrigir mensagens repetidas, danificadas ou perdidas. Outra função importante é controlar o fluxo de dados, evitando, por exemplo, que um transmissor rápido afogue um receptor lento.

Camada Rede

Ela determina o caminho que uma mensagem deverá fazer. O roteamento pode ser definido por uma tabela relacionando endereço lógico à endereço físico. Na interligação de várias redes, ela é responsável pela conversão dos endereços, que poderão ser diferentes. Outra função é o controle de congestionamento, determinando caminhos alternativos.

Camada Transporte

Esta camada oferece um serviço confiável (sem erros) fim a fim (sem preocupação com o caminho que é feito) e entrega as mensagens na ordem correta. Ela pode multiplexar várias conexões transparentes ao usuário. O Transporte é responsável pelo estabelecimento e encerramento de conexões.

Camada Sessão

Ela é responsável por estabelecer uma sessão entre máquinas diferentes. Um exemplo é a sincronização na transferência de dados, por exemplo, permitindo que uma transferência de um arquivo possa ser retomada do ponto que parou.

Camada Apresentação

Realiza funções de conversão de códigos como, por exemplo, ASCII e EBCDIC. É a camada responsável por permitir a comunicação entre máquinas diferentes. Outras funções são compressão de dados, criptografia e autenticação.

Camada Aplicação

É a camada de mais alto nível de abstração e oferece serviços para usuário como, transferência de arquivos, consulta a diretório e correio eletrônico.

1.5 Modelo de um protocolo

Um protocolo é o conjunto de regras que regulamentam a comunicação entre dois ou mais computadores. Na vida normal usamos protocolos de uma forma

natural, sem prestarmos atenção. Para que duas pessoas se comuniquem é necessário que elas tenham contato (físico ou telefone), precisam falar a mesma língua e precisamos construir frases adequadamente.

No mundo dos computadores é semelhante, os computadores precisam estar ligados fisicamente, com um cabo de rede local ou um par telefônico, falar a mesma linguagem e usar o mesmo protocolo (estrutura das mensagens). A cada camada de cada extremidade de comunicação é necessário que a mensagem seja idêntica, para permitir o entendimento.

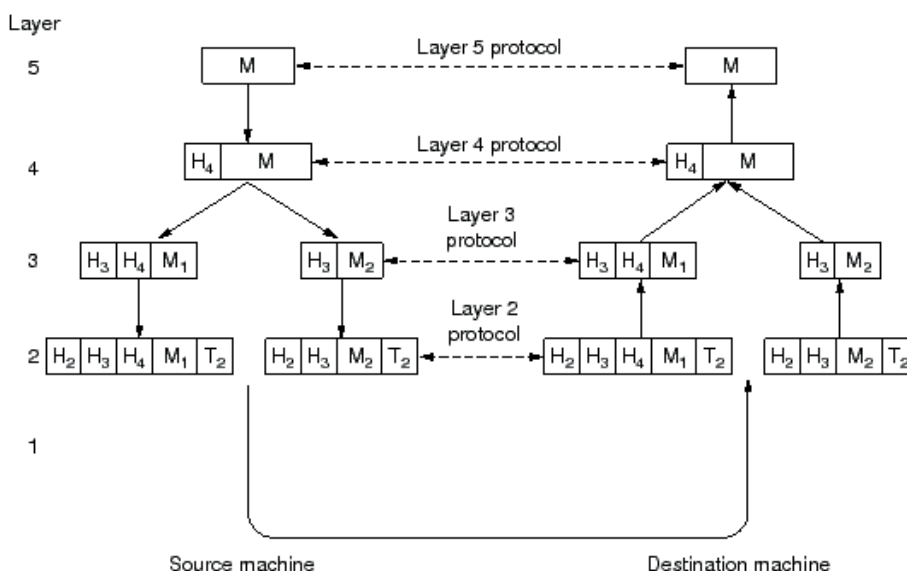



Figura 1.1.5: Exemplo de um protocolo entre computadores.

Na Figura 1.1.5 a mensagem M é entregue pela camada 5 à camada 4 para ser transmitida para a outra extremidade. Na camada 4 é colocado um cabeçalho (header) H4 para identificar a mensagem que será entregue à camada 3. A camada 3 não pode transmitir a mensagem M inteira, por isso ela é quebrada em dois pedaços, M1 e M2. Cada mensagem recebe um novo cabeçalho (header) H3 que indica a ordenação dos pacotes à outra extremidade, que deverá remontar a mensagem. A camada 2 adiciona um novo cabeçalho H2 e também uma terminação (trailer) T2 com um código de verificação para possibilitar que o destinatário verifique se não houve erro durante a transmissão. A mensagem é transmitida para o destino que realiza este processo no sentido inverso.

1.5.1 Exemplo: Protocolo TCP/IP

O TCP/IP (Transmission Control Protocol/Internet Protocol) foi inicialmente criado por pesquisadores da rede ARPA, e que mais tarde se tornou padrão

da rede Internet. A principal característica do TCP/IP é poder suportar a interligação de várias redes de diferentes tecnologias, podendo oferecer vários serviços a seus usuários, como por exemplo, o FTP, Telnet e o E-Mail. O TCP divide os dados em pacotes e cada pacote possui um número de sequência para remontar os dados novamente, além de informações que garantem o não corrompimento dos dados contidos no pacote.

O IP divide estes pacotes em partes menores ainda que além de ter os controles de remontagem e não corrompimento de dados, acrescenta informações de endereçamento de origem e destino. As as sub-redes podem dividir os pacotes IP e adicionar suas próprias informações de endereçamento, um pacote de IP pode passar por diversas sub-redes até atingir o endereço desejado de envio.

Mostramos a seguir na Figura 1.1.6 um diagrama da pilha de protocolos TCP/IP com vários protocolos de comunicação de dados segundo sua classificação por camadas.

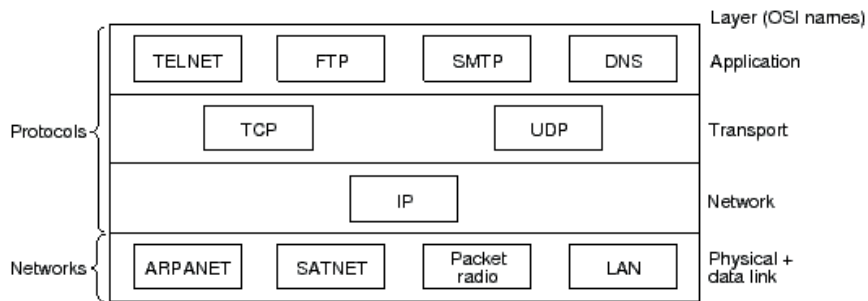



Figura 1.1.6 - Diagrama da pilha de protocolos TCP/IP

1.6 Organizações de Normatização

Os protocolos exigem um padrão rígido para possibilitar que diversos equipamentos, fabricados por diversos fabricante em países diferentes, possam se comunicar. Para isso existem três organizações principais responsáveis pela definição de normas de comunicação:

- IETF
- ISO
- ITU-T

1.6.1 Internet Engineering Task Force (IETF)

A normatização no meio Internet é conhecido por ser bastante livre e flexível. Qualquer pessoa pode criar uma norma e divulgá-la publicamente como Draft (rascunho). Este Draft é criticado, corrigido, adaptado, seguindo as sugestões

dadas pela comunidade. Após seis meses essa norma é apresentada ao IETF que julga a validade e relevância desta norma e analisa conflito com outras normas existentes. Caso seja aprovado este Draft recebe um número e se torna um RFC (Request for Comments). Se um RFC se mostra ser estável, tecnicamente competente, dispor de suporte público, ser reconhecido por boa parte da Internet e ter multiplas, independentes e interoperáveis implementações, é transformado em Norma Internet (Standard).

IETF (Internet Engeneering Task Force) - Organização responsável pela padronização e normatização da Internet

Em virtude do rápido avanço das tecnologias, dificilmente um RFC se torna uma Norma, por isso, a partir de seu reconhecimento com RFC a comunidade já passa a considerá-lo como norma de fato.

RFC (Request for Comments) - Segunda etapa da normatização na Internet, onde o documento já pode ser usado porém pode sofrer alterações.

1.6.2 International Organization for Standardization (ISO)

A ISO, fundada em 1946, é uma organização que congrega todas os orgão de normatização dos diversos países. Por exemplo, a ABNT é a organização brasileira filiada a ISO. Seu objetivo é tentar unificar todas as normas dos diversos membros. Foram publicadas mais de 5000 normas cobrindo desde dimensões de parafusos até energia solar. Uma norma importante foi a OSI que normatizou a arquitetura de comunicações.

O processo de publicação de uma norma ISO é bastante demorado, chegando a levar décadas. Como as redes de comunicações apresentam um desenvolvimento muito acelerado, este modelo acaba sendo preterido. Por isso o modelo Internet tem maior sucesso nesta área.

1.6.3 International Telecommunication Union - Telecommunications Sector (ITU-T)

O ITU-T, criado em 1993, é um órgão pertencente às Nações Unidas e substituiu o CCITT. Ele tem por objetivo normatizar as telecomunicações, como padrões sistema de telefonia, cobrança entre operadoras e padrões de operação de telecomunicações no mundo. A cada quatro anos o comitê se reúne e publica uma nova edição revisada de suas normas.

Atividades de avaliação

1. Quais as camadas do modelo OSI? Quais as funções de cada camada?
2. Qual a diferença do modelo Internet em relação ao modelo OSI? Quais camadas não existe no modelo Internet.
3. Qual a importância dos organismos normatizadores para a comunicação de dados.

2. Transmissão de dados

Qualquer transmissão de dados exige um meio físico para chegar ao destinatário. O sucesso de uma transmissão depende de dois fatores: a qualidade do sinal e a característica do meio de transmissão. O objetivo desse capítulo é apresentar uma introdução aos conceitos básicos e terminologia de transmissão de dados.

A Seção **2.1** apresenta as diversas topologias físicas de uma rede de comunicação de dados. A Seção **2.2** mostra as características de uma transmissão de dados. A Seção **2.3** apresenta as dificuldade de uma transmissão de dados como atenuação e ruído, e na Seção **2.4** o cálculo da capacidade de um canal. Finalmente, na Seção **2.5**, mostramos alguns meios físicos de transmissão de dados.

2.1 Topologias

A Topologia trata da distribuição geográfica de nós e arestas de uma rede. A topologia de uma rede depende do projeto das operações, da confiabilidade e do seu custo operacional. Ao se planejar uma rede, muitos fatores devem ser considerados, mas o tipo de participação dos nós é um dos mais importantes. Um nó pode ser fonte ou usuário de recursos, ou uma combinação de ambos.

Uma aresta ou ramo é uma trajetória de comunicação entre dois nós. O termo aresta é usado como sinônimo de canal ou circuito, e pode ser de vários tipos:

- Rádio
- Fibra ótica
- Satélite
- Cabo coaxial
- Linha telefônica

Um nó pode ser definido como qualquer ponto terminal de qualquer ramo da rede, ou a junção de dois ramos quaisquer. O hardware e o software de um nó depende de sua função principal.

Existem dois tipos básicos de rede: Ligação Ponto-a-ponto e Multiponto. Combinando-se os dois tipos básicos formam-se redes mais complexas, as chamadas Estruturas Mistas.

2.1.1 Ligação Ponto-a-Ponto

Nesta rede, o computador central é conectado a um equipamento de comunicação de entrada e saída por uma única linha.

Sempre que algum deles tiver algo a transmitir a linha estará livre, já que não há compartilhamento com outro equipamento. Nesta modalidade de ligação, o hardware conectado ao computador é o mais simples possível e o software de atendimento não precisa ser muito sofisticado.

2.1.2 Multiponto

Nesta modalidade de ligação existe sempre uma estação controladora que coordena o tráfico de dados das demais estações chamadas subordinadas. Este controle é feito através de uma rotina de atendimento denominada “POLL-SELECT”.

Estas redes podem permitir que estações subordinadas se comuniquem entre si diretamente ou apenas através da estação controladora. A diferença entre estes dois modos de envio de mensagens é a complexidade do controle.

2.1.3 Estruturas Mistas

As Estruturas Mistas são tipos de redes que utilizam características dos dois tipos básicos de redes, a ligação ponto-a-ponto e multiponto, para obter redes mais complexas e com maiores recursos. As estruturas mistas podem ser do tipo Barra, Estrela, Hierárquica, Anel e Distribuídas.

Barramento

Nesta configuração todos os nós (estações) se ligam ao mesmo meio de transmissão. A barra é geralmente compartilhada em tempo e frequência, permitindo transmissão de informação (Figura 1.2.1a).

Nas redes em barra comum, cada nó conectado à barra pode ouvir todas as informações transmitidas. Esta característica facilita as aplicações com mensagens do tipo difusão (para múltiplas estações).

Existe uma variedade de mecanismos para o controle de acesso à barra pode ser centralizado ou descentralizado. A técnica adotada para cada acesso à rede é a multiplexação no tempo. Em controle centralizado, o direito de acesso é determinado por uma estação especial da rede. Em um ambiente de controle descentralizado, a responsabilidade de acesso é distribuída entre todos os nós.

Nas topologias em barra, as falhas não causam a parada total do sistema. Relógios de prevenção ("watch-dog-timer") em cada transmissor devem detectar e desconectar o nó que falha no momento da transmissão.

O desempenho de um sistema em barra comum é determinado pelo meio de transmissão, número de nós conectados, controle de acesso, tipo de tráfego entre outros fatores. O tempo de resposta pode ser altamente dependente do protocolo de acesso utilizado.

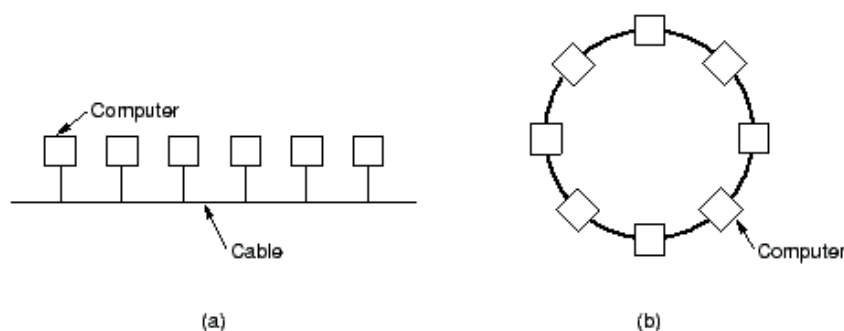



Figura 1.2.1: Topologias comuns em redes locais - barramento e anel.

Estrela

Neste tipo de rede, todos os usuários comunicam-se com um nó central, que tem o controle supervisor do sistema. Através deste nó central os usuários podem se comunicar entre si e com processadores remotos ou terminais. No segundo caso, o nó central funciona como um comutador de mensagens para passar os dados entre eles (Figura 1.2.1a).

O arranjo em estrela é a melhor escolha se o padrão de comunicação da rede for de um conjunto de estações secundárias que se comunicam com o nó central. As situações onde isto mais acontece são aquelas em que o nó central está restrito às funções de gerente das comunicações e a operações de diagnósticos.

O nó central pode realizar outras funções além das de chaveamento e processamento normal. Por exemplo, pode compatibilizar a velocidade de comunicação entre o transmissor e o receptor. Se o protocolo dos dispositivos fonte e destino utilizarem diferente protocolos, o nó central pode atuar como um conversor, permitindo duas redes de fabricantes diferentes se comunicar.

No caso de ocorrer falha em uma estação ou no elo de ligação com o nó central, apenas esta estação fica fora de operação. Entretanto, se uma falha ocorrer no nó central, todo o sistema pode ficar fora do ar. A solução deste problema seria a redundância, mas isto acarreta um aumento considerável dos custos.

A expansão de uma rede deste tipo de rede só pode ser feita até um certo limite, imposto pelo nó central: em termos de capacidade de chaveamento, número de circuitos concorrentes que podem ser gerenciados e números de nós que podem ser servidos.

O desempenho obtido numa rede em estrela depende da quantidade de tempo requerido pelo nó central para processar e encaminhar mensagens, e da carga de tráfego de conexão, ou seja, é limitado pela capacidade de processamento do nó central.

Esta configuração facilita o controle da rede e a maioria dos sistemas de computação com funções de comunicação possuem um software que implementa esta configuração.

Hierárquica

A topologia Hierárquica ou em árvore é essencialmente uma série de estrelas interconectadas. Geralmente existe uma estrela central onde outros ramos menores se conectam. A ligação entre nós é realizada através de derivadores e as conexões das estações realizadas da mesma maneira que no sistema estrela padrão (Figura 1.2.2c).

Cada ramificação significa que o sinal deverá se propagar por dois caminhos diferentes. A menos que estes caminhos sejam perfeitamente casados, os sinais terão velocidades de propagação diferentes e refletirão os sinais de diferentes maneiras. Por este motivo, em geral, as redes hierárquicas trabalham com taxas de transmissão menores do que as redes de barramento comuns.

Esta topologia é muito usada para supervisionar aplicações de tempo real, como algumas de automação industrial e automação bancária.

Pequenos sistemas baseados em mini ou microcomputadores proporcionam o atendimento em tempo real das atividades da agência bancária. Quando uma operação exige acesso a informações que não estão disponíveis na agência, elas são buscadas no computador central. Se este não tiver acesso direto a estas informações, redirecionará a busca para outro computador da rede que as detém.

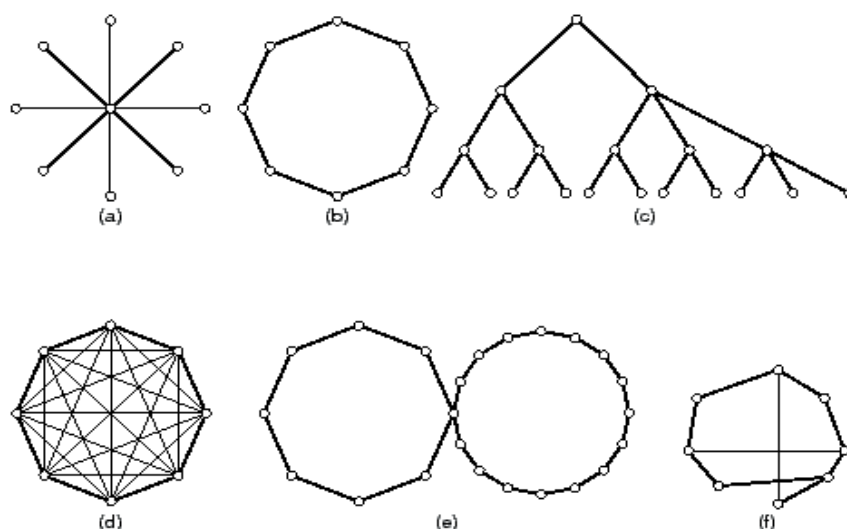



Figura 1.2.2: Topologias comuns em redes ponto-a-ponto.

Anel

Uma rede em anel consiste de estações conectadas através de um caminho fechado. Nesta configuração, muitas das estações remotas conectadas ao anel não se comunicam diretamente com o computador central (Figura 1.2.1b e Figura 1.2.2b).

Redes em anel são capazes de transmitir e receber dados em qualquer direção, mas as configurações mais usuais são unidirecionais, de forma a tornar menos sofisticado os protocolos de comunicação que asseguram a entrega da mensagem corretamente e em sequência ao destino.

Quando uma mensagem é enviada por um nó, ela entra no anel e circula até ser retirada pelo nó destino, ou então até voltar ao nó fonte, dependendo do protocolo empregado. O último procedimento é mais desejável porque permite o envio simultâneo de um pacote para múltiplas estações. Outra vantagem é a de permitir a determinadas estações receber pacotes enviados por qualquer outra estação da rede, independentemente de qual seja o nó destino.

Os maiores problemas desta topologia são relativos a sua pouca tolerância a falhas. Qualquer que seja o controle de acesso empregado, ele pode ser perdido por problemas de falha e pode ser difícil determinar com certeza se este controle foi perdido ou decidir qual nó deve recriá-lo. Erros de transmissão e processamento podem fazer com que uma mensagem continue eternamente a circular no anel. A utilização de uma estação monitora pode contornar estes problemas. Outras funções desta estação seriam: iniciar o anel, enviar pacotes de teste e diagnóstico e outras tarefas de manutenção. A estação monitora pode ser dedicada ou uma outra que assuma em determinado tempo essas funções.

Esta configuração requer que cada nó seja capaz de remover seletivamente mensagens da rede ou passá-las adiante para o próximo nó. Nas redes unidirecionais, se uma linha entre dois nós cair, todo o sistema sai do ar até que o problema seja resolvido. Se a rede for bidirecional, nenhum ficará inacessível, já que poderá ser atingido pelo outro lado.

Distribuída

Esta configuração consiste de vários pontos de concentração, cada um com seu conjunto próprio de terminais geograficamente concentrados. As ligações são estabelecidas apenas entre estes pontos de concentração, o que diminui consideravelmente o custos das linhas. Só estas linhas precisarão ter uma capacidade muito maior de transmissão para poder atender às requisições de comunicação exigidas pelos seus terminais.

Para se garantir que, em caso de falha de linhas entre pontos centralizadores, as transmissões não serão interrompidas, é comum a conexão destes centros a mais de um outro centro. Outra forma de redundância de linhas é a conexão de cada ponto central a todos os demais pontos de concentração. Nesta rede, denominada completamente conectada (Figura 2.2d), a probabilidade de estrangulamento nos horários de pico de tráfego é muito baixa e sua confiabilidade é muito maior. O problema é o altíssimo custo das linhas.

Outra alternativa seria uma rede parcialmente conectada (Figura 1.2.2d), onde se consegue alguma redundância sem um custo de comunicação alto.

2.2 Características de Transmissão de Dados

Algumas características ajudam a classificar uma transmissão de dados. São elas: sentido da transmissão, modo de transmissão e tipos de enlace.

2.2.1 Sentido de Transmissão

Uma comunicação pode ser classificada segundo o sentido da transmissão em simplex, semi-duplex (half-duplex) e duplex (full-duplex). A comunicação simplex ou unidirecional se dá em um único sentido enquanto a semi-duplex ou bidirecional se dá nos dois sentidos, porém não simultaneamente. A comunicação duplex ou bidirecional simultânea permite o tráfego de informações simultâneas nas duas direções.

2.2.2 Modo de Transmissão

Segundo uma classificação espacial a transmissão pode ser série ou paralela. A transmissão paralela é normalmente usada para pequenas distâncias den-

tro de um computador (por exemplo, barramento de dados) ou ainda para conectar periféricos próximos (por exemplo, uma impressora). Sua vantagem é a velocidade de transmissão pois vários bits são transmitidos simultaneamente. Para grandes distâncias a transmissão série é mais empregada pois permite uma grande economia em relação ao suporte de transmissão.

Em relação ao tempo (classificação temporal) a transmissão pode ser síncrona ou assíncrona. Na transmissão síncrona o relógio (clock) é enviado juntamente com sinal transmitido, permitindo o aproveitamento total da banda de comunicação. Na transmissão assíncrona o relógio não é enviado junto ao sinal, obrigando a inclusão de bits de sincronismo (start bit e stop bit) provocando uma perda no aproveitamento da banda.

2.2.3 Tipo de enlace

Os equipamentos de comunicação de dados podem ser conectados através de diferentes tipos de enlace. O mais comum é a ligação ponto-a-ponto. Os dois outros tipos de enlace são o ponto-a-multiponto, muito usado em redes locais e de satélites, e o multiponto-a-ponto, usado em aplicações de consulta a bancos de dados. A ligação de conferência (multiponto-a-multiponto) é um tipo de enlace que vem recebendo importância crescente devido às aplicações em ensino e trabalho cooperativo. Finalmente, o enlace de difusão (broadcast) onde todos os equipamentos recebem informações.

2.3 Dificuldades na transmissão

Como qualquer meio da natureza, uma transmissão apresenta algumas dificuldades que precisam ser consideradas para atingir o objetivo final: comunicar.

2.3.1 Notação decibel

Muitas vezes a relação entre sinal de entrada e saída, ou sinal transmitido e recebido é mais importante que o valor do sinal propriamente dito. Por isso é comum representar a relação de potência de sinal com a notação decibel, mostrada na Equação:

$$Decibel = 10 \log_{10} \frac{S}{E}$$

Onde, S é a potência do sinal de saída e E a potência do sinal de entrada. O uso de logaritmo é para diminuir o tamanho dos números quando o ganho/perda forem muito grandes. Note que se o sinal de saída for maior que o de entrada (um amplificador, por exemplo) o valor em decibel é positivo enquanto se a saída for menor que a entrada (medida de atenuação, por exemplo) o valor em decibel é negativo.

2.3.2 Atenuação de um sinal de comunicação

Qualquer sinal transmitido perde energia durante seu caminho até o receptor. Este fator é importante pois classifica os meios de transmissão para cada tipo de uso. Por exemplo, um material que oferece baixa perda de potência é o mais indicado para transmissão de longa distância A atenuação também é proporcional a frequência do sinal, isto é, para um mesmo material a atenuação de um sinal de frequência mais alta é maior que o sinal de frequência mais baixa. Como um sinal digital tem componentes de diversas frequências (Fourier), essa diferença de atenuação pode provocar erros na interpretação do sinal no receptor.

A atenuação geralmente é representado pela notação de decibel.

2.3.3 Distorção por atraso

Um atraso diferente para diferentes frequências pode provocar erros na interpretação dos dados no receptor, por causa da série de Fourier.

2.3.4 Ruído

O ruído faz parte do meio ambiente, e quando está próximo da linha de comunicação ele pode causar erros na interpretação dos dados no receptor.

2.4 Capacidade de um Canal de Comunicação

2.4.1 Lei de Nyquist

Todo sistema de comunicação procura tirar o máximo proveito do seu canal de comunicação transmitindo na sua taxa de transmissão máxima. Com a finalidade de determinar a taxa de transmissão máxima em um canal sem ruído, H. Nyquist, em 1924, demonstrou que um sinal com banda passante W Hz pode representar uma sequência de dados de 2 W. Se considerarmos que o sinal pode ter V níveis discretos, o Teorema de Nyquist prova que a capacidade máxima C do canal é dada pela Equação:

$$C = 2W \log_2 V \ bps$$

Logo, um canal de voz de 3 kHz (linha telefônica) não pode transmitir sinal binário (V=2) a uma taxa maior que 6.000 bps. Em um sistema de comunicação com 16 níveis (V=16) poderia se transmitir informações a uma taxa de 24.000 bps.

2.4.2 Lei de Shanon

Claude Shanon, em 1948, estendeu o trabalho e Nyquist para o caso de ruído gaussiano (ruído branco) e provou que a capacidade máxima do canal é dada pela Equação:

$$C = W \log_2 \left(1 + \frac{S}{N}\right) bps$$

A expressão S/N é chamada de relação sinal ruído e indica a potência do sinal S em relação a potência do ruído N. Esta relação geralmente é fornecida em decibéis (dB) e corresponde a 10 log S/N. Por exemplo, uma relação S/N de 100 é igual a 20 dB e de 1.000 é igual a 30 dB.

Assim, a linha telefônica com banda passante 3 kHz e com uma relação sinal ruído de 30 dB (valor normalmente aceitável) encontramos uma capacidade C= 30 kbps.

2.5 Meios Físicos

As telecomunicações utilizam uma vasta largura do espectro eletromagnético, cada um utilizando um meio de transmissão adequado. A Figura 1.2.3 mostra o espectro eletromagnético usado em comunicações.

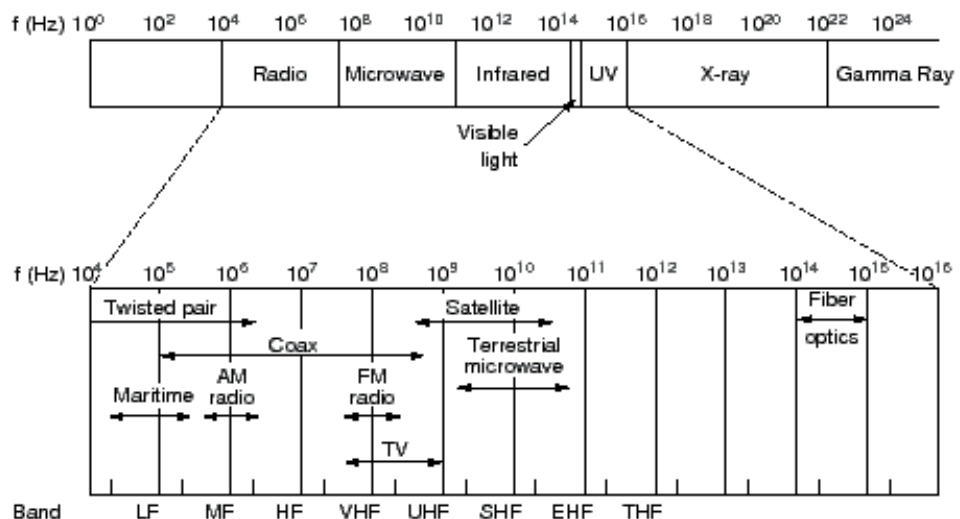



Figura 1.2.3: Espectro eletromagnético de telecomunicações.

2.5.1 Par trançado

O par trançado é composto de um ou mais pares de fios metálicos (normalmente de cobre) isolados e enrolados em forma espiral (Figura 1.2.4).

O trançado dos fios permite diminuir os efeitos de indução de corrente em um dos condutores devido ao campo elétrico inverso criado pelo outro condutor. Ele é usado como suporte de transmissão na rede telefônica e em cabeamento de rede local.

O par metálico trançado é um suporte de transmissão de baixo custo, alta maleabilidade, peso e dimensões reduzidas, fácil manuseio, permite conexões bastantes simples e apresenta interfaces de baixo custo.

Um cabo de par trançado pode ser do tipo blindado ou não blindado.

O cabo blindado, também conhecido como STP tem uma membrana de alumínio envolvendo todos os pares trançados ou uma membrana fazendo uma blindagem individual para cada par. Isso reduz o interferência do meio ambiente e também reduz a interferência entre pares (crosstalk) quando isolado individualmente.

O cabo não blindado, também conhecido como UTP, consiste em apenas um conjunto de pares trançados entre si. Pelo fato de os pares serem trançados muito próximos, uma interferência eletromagnética externa atuando em um lado da trança compensa a interferência do outro lado da trança. Esse engenhoso mecanismo cria uma autoproteção eletromagnética, protegendo o sinal de interferências externas, sem a necessidade de usar uma blindagem externa.

(a) (b)

Figura 1.2.4: Cabo par trançado.

2.5.2 Cabo Coaxial

Assim como o par trançado, o cabo coaxial também é composto de dois condutores metálicos. No entanto, sua geometria é particular (Figura 1.2.5) pois os condutores estão dispostos em forma concêntrica e separados por um dielétrico (isolante). A grande vantagem desta configuração é evitar a radiação de energia uma vez que o campo elétrico fica confinado no interior do cabo. Desta forma, o cabo coaxial suporta frequências e distâncias maiores que o par trançado. Além de não irradiar energia (não provoca interferência em outros equipamentos) o seu condutor externo age como uma blindagem à interferências eletromagnéticas externas.

Existe uma grande variedade de cabos coaxiais que diferem segundo a impedância característica, área dos condutores e material do dielétrico e encapamento.

Copper core
Insulating material
Braided outer conductor
Protective plastic covering

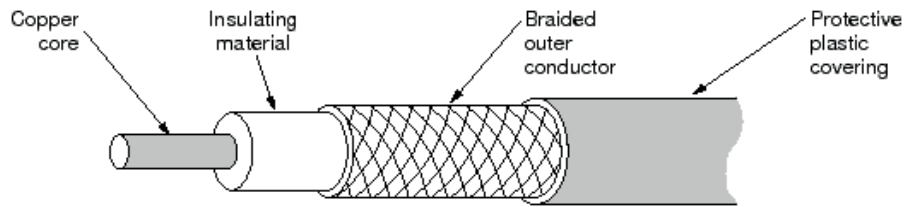



Figura 1.2.5: Cabo coaxial.

2.5.3 Fibras Óticas

As primeiras experiências de transmissão de luz em fibras de vidro foram realizadas em 1930 por Lamb. No entanto apenas na década de 60 foi possível transmitir informações por uma fibra ótica a uma distância relativamente grande (Figura 1.2.6). Atualmente já são fabricadas fibras óticas com atenuação muito baixa que possibilitou a transmissão por longas distâncias sem necessidade de repetidores.

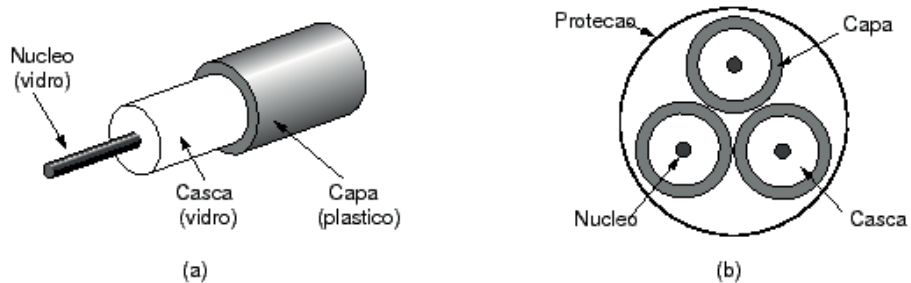



Figura 1.2.6: Fibra ótica.

A Figura 1.2.7 apresenta o gráfico de atenuação de uma fibra ótica. Podemos notar que há três faixas de frequência que podem ser utilizadas: a faixa de 0,85μ, atualmente em desuso, a faixa de 1,3μ e a faixa de 1,55μ, que apresentam a menor atenuação e são as mais utilizadas.

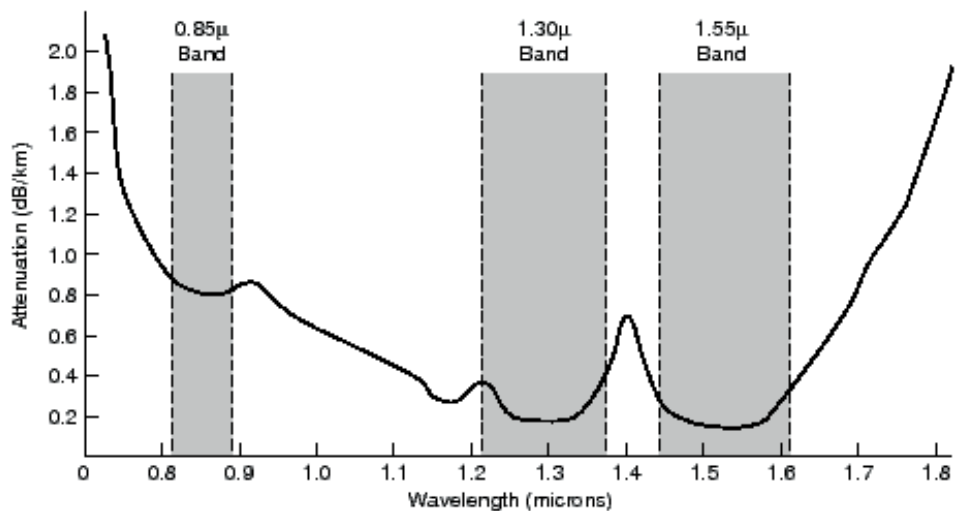



Figura 1.2.7: Atenuação em uma fibra ótica.

As fibras óticas apresentam características próprias que tornam um meio de transmissão bastante vantajoso em relação aos outros meios de transmissão. Entre as vantagens podemos citar:

1. Banda passante larga. A transmissão em fibras óticas é realizada na faixa de 100 à 1.000 THz o que significa capacidade de transmissão muito grande. É comum fibras óticas comerciais com capacidade de transmitir 20 Gbits muito em breve deverá ser atingida taxas na ordem de Tbits.
2. Atenuação baixa. Curiosamente a atenuação foi o principal problema para utilização das fibras óticas, porém atualmente consegue-se atenuações menores de 0.1 dB/Km, que permitem a colocação de repetidores com intervalos de 50 a 100 Km.
3. Isolação elétrica, Imunidade e interferências a ruídos. Por ser construída utilizando apenas materiais dielétricos (silício) as fibras óticas não sofrem interferência eletromagnética. Além disso não existe problema de aterramento no interfaceamento dos transceptores. O rompimento de uma fibra ótica não provoca faísca, permitindo sua utilização em ambientes explosivos, como indústria de petróleo e mineração. Como não sofre interferência eletromagnética não sofre com a proximidade de motores elétricos, descargas atmosféricas, possibilitando sua instalação junto às linhas de transmissão de energia elétrica ou leito de ferrovias. O excelente confinamento do sinal luminoso permite a construção de cabos com múltiplas fibras sem haver interferências entre elas. Peso e tamanho reduzidos.
4. O pequeno peso e a grande banda passante possibilita a construção de cabos significativamente menores e mais leves que os cabos equivalentes em cobre.

As principais desvantagens são:

1. Custo e tecnologia. Embora a fibra ótica seja feita a partir de sílica, material abundante na crosta terrestre, o processo de purificação é bastante custoso. Além disso a fragilidade mecânica exige tecnologia de encapsulamento sofisticada que encarecem o custo do cabo. A mão de obra necessária para instalar uma conexão é especializada. As interfaces óticas também são muito mais caras que as interfaces de cabos metálicos. Mesmo assim, a alta capacidade de transmissão compensa os custos elevados e cada vez mais a fibra ótica tem se tornado o meio principal de telecomunicações.
2. Custo de manutenção. As reduzidas dimensões provocam dificuldade na realização de emendas, aumentando o custo de operação.

3. Inadaptada para sistemas multiponto. Uma ligação de fibra ótica é basicamente ponto-a-ponto, dificultando a construção de sistemas multiponto.

2.5.4 Radiofreqüência

A transmissão por radiofrequência não necessita de meio físico de transmissão, por isso é muito usado em transmissão para grandes áreas ou regiões remotas desprovidas de facilidade de comunicação. A transmissão pode ser terrestre, onde um ponto se comunica com outro através de micro-ondas, ou espacial, onde o retransmissor é um satélite em órbita da terra.

A comunicação terrestre pode utilizar frequências baixa, na faixa do VHF, onde o sinal é refletido na ionosfera (Figura 2.8b). Essa tecnologia tem alcance grande (100 a 500 Km) mas a velocidade é baixa (alguns Kbps). A outra forma é utilizar frequências altas, na faixa de micro-ondas onde permite altas taxas de transmissão (na ordem de Mbps) porém o alcance é limitado à visada das antenas (até 20 Km). Geralmente é usada modulação Spread Spectrum que garante confiabilidade e sigilo nas transmissões (Figura 1.2.8a).

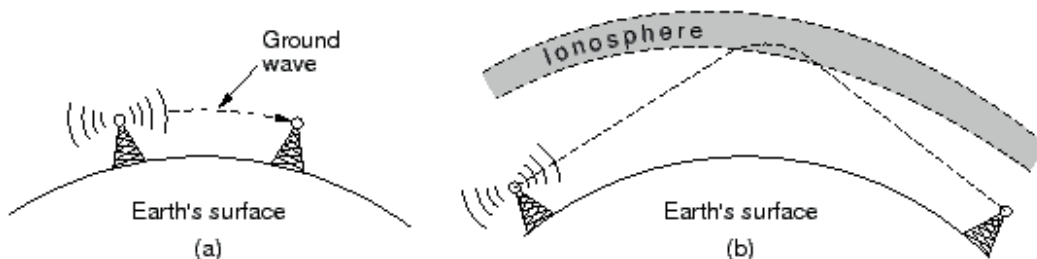



Figura 1.2.8: Transmissão por radiofreqüência terrestre (Microondas e VHF).

Comunicação via satélite

Para tentar resolver a limitação do alcance do rádio de alta frequência mantendo-se uma alta taxa de transmissão é a utilização de satélites. Em virtude de estar em uma grande altitude ele permite a comunicação entre dois pontos sem visada (desde que ambos tenham visada com o satélite).

A Figura 1.2.9 mostra os três tipos de satélite de acordo com a altitude. Os satélites geoestacionários (GEO) mantém sua posição no céu, porém sua grande altitude provoca altos retardos que dificultam a comunicação. Poucos satélites conseguem cobrir todo o globo terrestre.

Os satélites de órbita baixa (LEO) não ficam na mesma posição do céu e a comunicação é realizada com o satélite mais próximo. Seu funcionamento é semelhante ao telefone celular, exigindo um controle mais complexo para

realizar a conexão. Como sua altitude é baixa, os retardos são baixos, semelhantes aos retardos de redes terrestres. Para cobrir todo o globo é necessário uma grande quantidade de satélites e, por causa do atrito com as camadas de ar da Terra, sua vida útil é bastante reduzida.

Os satélites de órbita média (MEO) são intermediários aos GEO e LEO, apresentados vantagens e desvantagens intermediárias.

Um exemplo de comunicação por satélite é a tecnologia VSAT, onde uma estação central de maior potência (hub) reduz o tamanho das estações remotas.

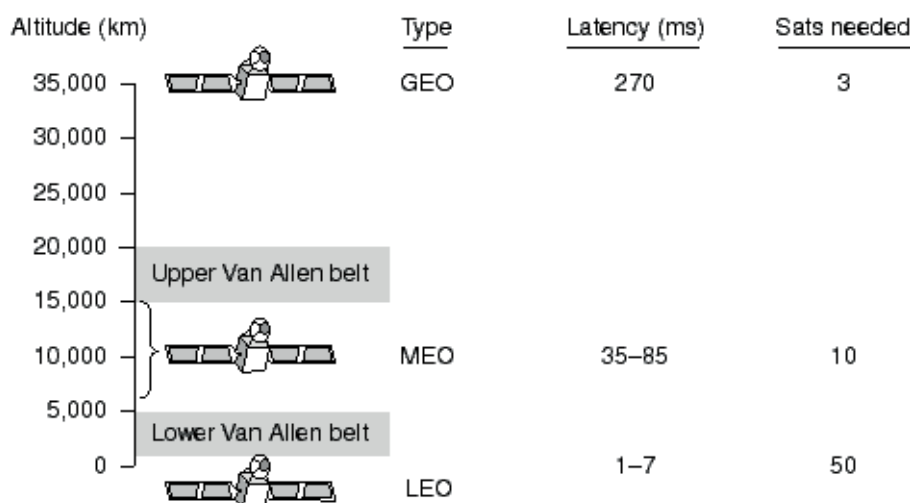



Figura 1.2.9: Transmissão por radiofrequência via satélite.

Atividades de avaliação

1. Cite as principais topologias usadas em redes de comunicação. Exemplifique graficamente.
2. Quais são as principais dificuldades para a transmissão de dados e quais os efeitos que ela pode causar.
3. Considere o Teorema de Nyquist. Qual a taxa de transmissão máxima (em bps) de um sistema de comunicação que tem um canal de 4 KHz e 1024 níveis de tensão para representar um símbolo. Idem para níveis binários.
4. Qual a capacidade máxima de transmissão binária, dada pelo teorema de Shanon, para um canal telefônico de 4 KHz de banda passante e 10 dB de relação sinal ruído? Idem para 20 dB e 30 dB.
5. Qual a capacidade de um canal de teleimpressora com 300 Hz de banda passante e relação sinal ruído 3 dB.

6. Cite as vantagens e desvantagens do uso de satélite geoestacionário como meio de comunicação.
7. Você é responsável pelo projeto de rede local em uma empresa e deve escolher qual tipo de cabo deve utilizar: Par Trançado, Coaxial, Fibra Ótica ou Sem fio. Considere os quesitos de confiabilidade e o menor custo. Justifique suas respostas.
   a) **Indústria Petroquímica.** Longa distância (>1000m) e alta densidade de equipamentos elétricos.
   b) **Oficina Mecânica.** Média distância (<200m), relativa densidade de equipamentos elétricos e tubulação antiga.
   c) **Escritório de Advocacia.** Curta distância (<100m), poucos equipamentos elétricos.
   d) **Canteiro de Obras.** Duto subterrâneo alagado na época da chuva, longa distância, nenhum equipamentos elétricos próximo.
   e) **Siderúrgica.** Longa distância, alta densidade de equipamentos elétricos, tráfego de caminhões pesados e ambiente sujo (pó e fumaça).

3. Codificação de Dados

Um dado na sua forma pura nem sempre é ideal para ser transmitido por um meio de comunicação real. Esse capítulo mostra diversas técnicas para codificação de dados. A seção 3.1 apresenta várias técnicas de codificação digita e analógica e a seção 3.2 apresenta a codificação spread-spectrum. Finalmente, apresentamos na seção 3.3 as técnicas de multiplexação.

3.1 Introdução à Codificação de Dados

A informação digital ou analógica que sai de uma interface nem sempre é a forma ideal para ser transmitido através de um meio de comunicação. Por isso é necessário aplicar uma transformação neste sinal. Se a informação for digital e o meio analógico é necessário converter o dado digital em sinal analógico, usando um equipamento chamado modem. Para cada transformação existem várias técnicas que são mostradas a seguir.

3.1.1 Dado Digital Sinal Digital

O primeiro tipo de codificação é o digital-digital e é mostrado na Figura 1.3.1. A codificação mais simples é transmitir um sinal digital puro por uma linha de transmissão, no qual é chamado de NRZ. A grande vantagem é que a banda de transmissão é aproveitada ao máximo, mas pode apresentar sinal DC

quando o dado apresenta muitos uns ou zeros, causando erros na identificação na extremidade oposta. Outro problema é a falta de sincronização causando também erro de identificação. A codificação NRZ somente é usada em velocidades e frequências baixas como gravação digital em mídia magnética.

Um outro grupo de codificação é chamada bifásica, que resolve as limitações do NRZ. Um exemplo é a codificação Manchester e a Manchester Diferencial mostrada na Figura 1.3.1. Na codificação Manchester sempre há uma transição no meio de cada período que serve como relógio do sinal. Uma transição positiva (de zero para um) representa o dígito 1 e uma transição negativa (de um para zero) representa o dígito 0. No Manchester Diferencial somente a posição da transição é utilizada, quando houver transição no início do período representa dígito 0 e se não houver transição no início do período representa dígito 1.

A codificação bifásica apresenta várias vantagens:

1. Sincronização. Como há uma transição em cada período o receptor ficará sempre sincronizado, por isso o código bifásico é conhecido como self-clocking (relógio auto-regenerado).
2. Sem componente DC. Observando a forma de onda de um código bifásico podemos concluir que não há componente DC.
3. Detecção de erro. A ausência de uma transição esperada pode ser usada para detecção de erro e um ruído tem que gerar uma inversão de dois sinais consecutivos para provocar um bit errado no receptor.

A desvantagem da codificação bifásica é que a frequência do sinal deverá ser o dobro da taxa de transmissão, diminuindo a capacidade do canal. A codificação Manchester é utilizada na rede Ethernet (CSMA/CD) e o Manchester Diferencial é usado na rede Token Ring (IEEE 802.5).

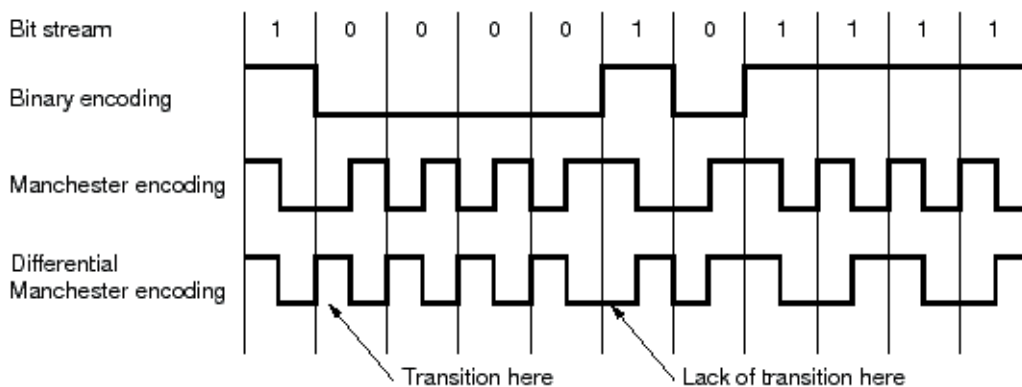



Figura 1.3.1: Codificação digital-digital.

3.1.2 Dado Digital Sinal Analógico

Uma linha telefônica transmite apenas sinal analógico, então para se transmitir um dado digital é necessário convertê-lo em sinal analógico. Esta função é realizada pelo modem.

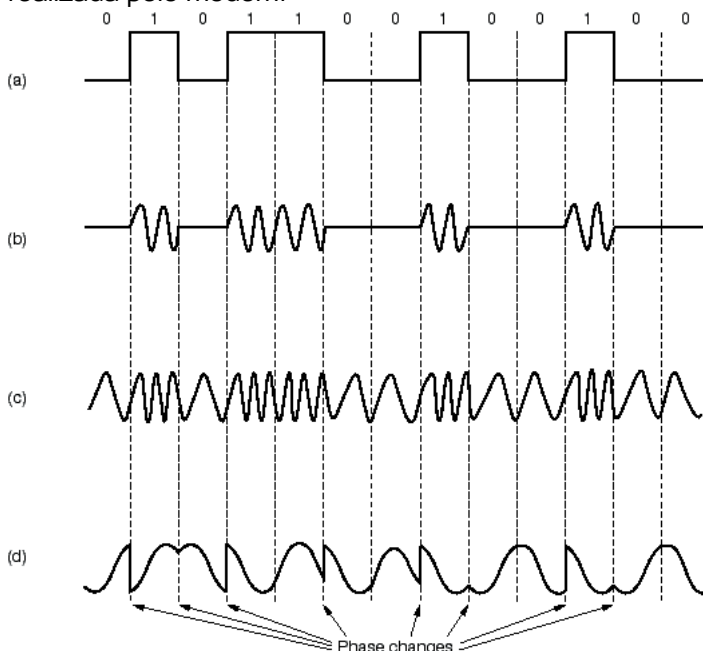



Figura 1.3.2: Codificação digital-analógica.

A primeira forma é a modulação em amplitude, mostrado na Figura 1.3.2b. Quando o dado for o bit 0 nenhum sinal é transmitido e se o bit for 1 é transmitida a portadora do sinal. Esta forma apresenta muito erro porquê qualquer ruído pode causar o entendimento errado de um bit.

A segunda forma é a modulação em frequência, mostrado na Figura 1.3.2c. Quando o dado for o bit 0 é transmitido um sinal com frequência f1 se o bit for 1 é transmitida um sinal com frequência f2. Com esta forma se consegue menos erros do que na modulação em amplitude, porém a capacidade de transmissão é reduzida, no máximo 1200 bps em uma linha telefônica.

A terceira forma é a modulação em fase, mostrado na Figura 1.3.2d. Quando o dado for o bit 0 é transmitido um sinal com fase $\theta 1$ e se o bit for 1 é transmitida um sinal com fase. Esta forma é muito semelhante a modulação por frequência e possibilita maior capacidade de transmissão, chegando a 33.200 bps em uma linha telefônica. A primeira forma é a modulação em amplitude, mostrado na Figura 1.3.2b. Quando o dado for o bit 0 nenhum sinal é transmitido e se o bit for 1 é transmitida a portadora do sinal. Esta forma apresenta muito erro porquê qualquer ruído pode causar o entendimento errado de um bit.

A segunda forma é a modulação em frequência, mostrado na Figura 1.3.2c. Quando o dado for o bit 0 é transmitido um sinal com frequência f1 se o bit for 1 é transmitida um sinal com frequência f2. Com esta forma se consegue menos erros do que na modulação em amplitude, porém a capacidade de transmissão é reduzida, no máximo 1200 bps em uma linha telefônica.

A terceira forma é a modulação em fase, mostrado na Figura 1.3.2d. Quando o dado for o bit 0 é transmitido um sinal com fase $\theta 1$ e se o bit for 1 é transmitida um sinal com fase. Esta forma é muito semelhante a modulação por frequência e possibilita maior capacidade de transmissão, chegando a 33.200 bps em uma linha telefônica.

3.1.3 Dado Analógico Sinal Digital

Ao longo dos últimos 40 anos foram marcados pela contínua digitalização das redes de comunicação, melhorando a qualidade do sinal recebido aproveitando a melhor imunidade a ruído do meio digital. Um problema sério é converter um dado analógico em sinal digital, pois por melhor que seja sempre há uma perda de informação.

A primeira técnica é chamada PCM mostrada na Figura 31..3. Ela consiste em amostrar o sinal analógico com um período constante, medir o valor amostrado e converter esse valor para um número digital. A voz humana, com uma faixa de frequência abaixo de 4 KHz, é amostrada a uma taxa de 8000 vezes por segundo. Esse valor amostrado é comparado com uma escala de 256 níveis (8 bits) o que exige uma taxa de transmissão de 64000 bps, que é a banda utilizada para canal de voz digitalizado não comprimido. A técnica PCM é sem dúvida a mais utilizada atualmente no sistema telefônico.

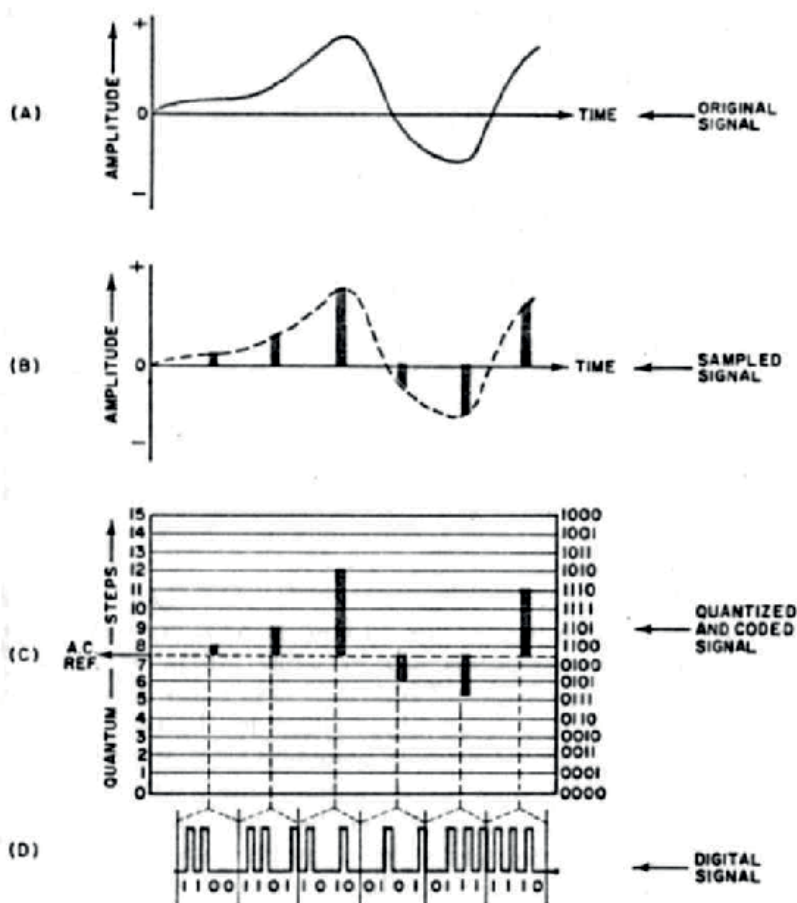



Figura 1.3.3: Modulação PCM.

Uma outra técnica é chamada Modulação Delta, mostrada na Figura 1.3.4. Esta técnica assume que um sinal analógico sofre pequenas variações em um pequeno intervalo de tempo, assim cada bit transmitido indica um acréscimo ou decréscimo do sinal anterior. Estudos matemáticos demonstram que a Modulação Delta consegue recuperar um sinal de voz (4KHz) com qualidade excelente usando apenas 9000 bps, enquanto o PCM necessita 64000 bps para se obter a mesma qualidade. Muitas outras técnicas tem surgido ao longo dos anos e acreditamos que sejam usados em breve nos equipamentos utilizados por nós (a Modulação Delta é utilizada nos roteadores VoIP).

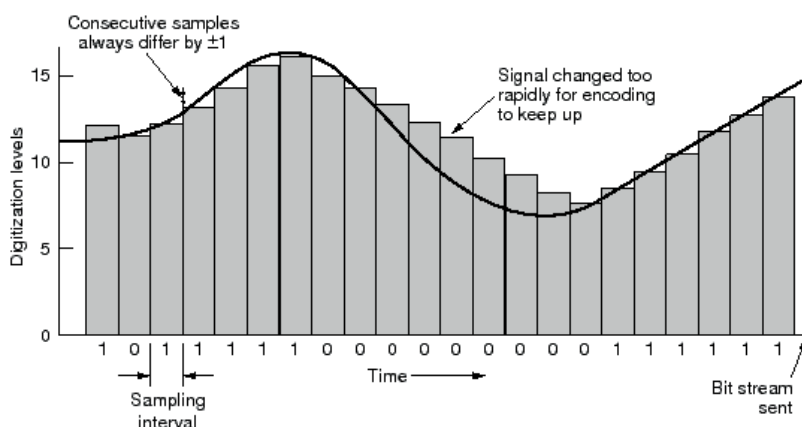



Figura 1.3.4: Modulação Delta.

3.1.4 Dado Analógico Sinal Analógico

Esta é a codificação mais antiga, mais ainda é usada apesar da digitalização das redes de comunicação. Existem duas formas de modulação analógica-analógica.

Modulação em Amplitude. A portadora de transmissão é tem a amplitude modulada em função do dado a ser transmitido. É a técnica usada nas rádios AM.

Modulação em Frequência ou Fase. A portadora de transmissão é tem a frequência (ou fase) modulada em função do dado a ser transmitido. É a técnica usada nas rádios FM.

3.2 Codificação Spread Spectrum

Durante a Segunda Guerra Mundial foi usado um rádio que mudava de canal a cada fração de segundo para impedir a interceptação pelo inimigo. O rádio receptor precisava conhecer a sequência de mudança para possibilitar o entendimento da mensagem. Essa técnica foi mantida em segredo até meados da década de 70, quando foi permitido construir equipamentos civis utilizando

esta técnica. A grande vantagem do Spread Spectrum é a grande quantidade de combinações de canais que possibilita a utilização privativa por vários usuários simultaneamente.

Mostramos na Figura 1.3.5 um exemplo de modulação Spread Spectrum. Vamos considerar que a operação de cálculo é um OU exclusivo e que na primeira linha mostra os o dado que queremos transmitir. A segunda linha mostra uma sequência de código que é conhecido pelo transmissor e receptor. A terceira linha mostra o resultado da operação OU exclusivo que é transmitida para o receptor.

O receptor conhece a sequência de código e aplica no sinal codificado recebido do transmissor. Aplicando a operação OU exclusivo conseguimos recuperar o sinal original.

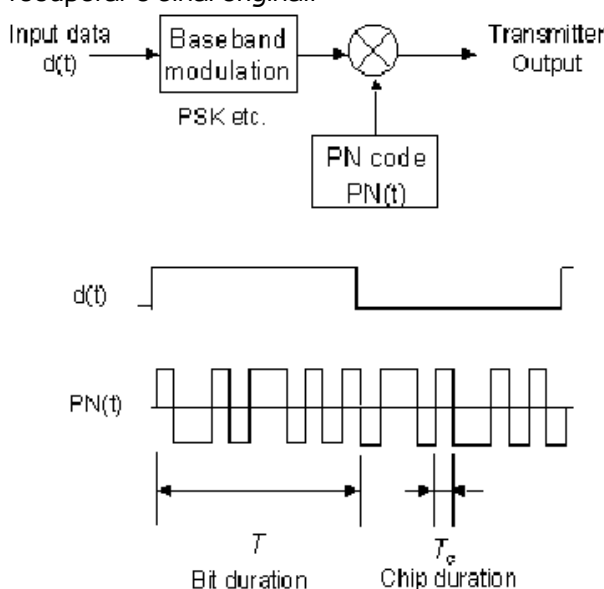



Figura 1.3.5: Exemplo de codificação Spread Spectrum.

A técnica de Spread Spectrum é muito usada na telefonia celular (CDMA) e nos equipamentos de rede sem fio (IEEE 802.11).

Existem dois tipos de modulação Spread Spectrum: Direct Sequence e Frequence Hoop.

3.2.1 Spread Spectrum Direct Sequence

Neste caso apenas uma frequência é utilizada e a codificação é realizada como mostrado na Figura 3.5. Esta técnica apresenta alta velocidade (chegando a 54 MBPS no IEEE 802.11g) e latências baixas (10 ms), mas é mais sensível a interferência eletromagnética, por isso recomendado apenas para ambientes internos (rede local sem fio).

3.2.2 Spread Spectrum Frequence Hoop

Neste caso o sinal transmitido muda de frequência de acordo com o código de transmissão. Esta técnica apresenta velocidades menores (no máximo 3 MBPS) e latências altas (200 ms), porém é mais resistente à interferências eletromagnéticas e por isso recomendado para ambientes externos (interligação entre prédios).

3.3 Multiplexação

Compartilhamento de um meio entre vários canais.

Um meio físico precisa transmitir informação de mais de um usuário. As técnicas de multiplexação são usadas para possibilitar a mescla e recuperação de vários sinais transmitidos. O diagrama geral de multiplexação é mostrada na Figura 1.3.6.

Figura 1.3.6: Diagrama genérico de Multiplexação.

3.3.1 Multiplexação por divisão de frequência (FDM)

A multiplexação em frequência (Figura 1.3.7) é a mais antiga e é mais apropriada para equipamentos analógicos. Cada canal utiliza um canal que sofre uma translação de frequência e é transmitido juntamente com os outros canais. Na outra extremidade os canais são separados com filtros e o sinal é recuperado.

Esta técnica ainda é usada, mas apenas para equipamentos antigos, pois a maioria dos equipamentos novos tem usado a multiplexação TDM.

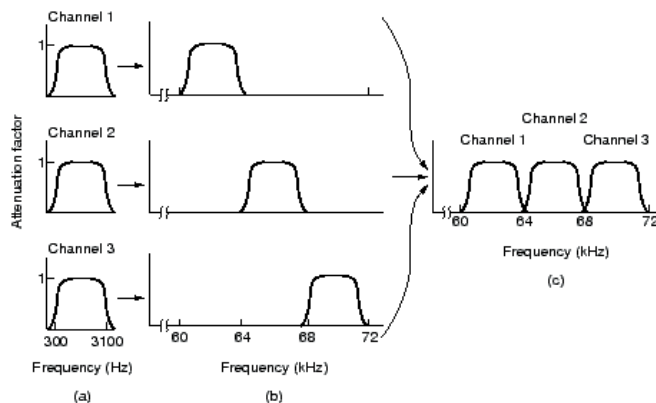



Figura 1.3.7: Multiplexação na frequência (FDM).

3.3.2 Multiplexação por divisão do tempo (TDM)

A multiplexação no tempo (Figura 1.3.8) é a mais utilizada atualmente e exige equipamentos digitais. Cada canal utiliza uma fração do tempo do pacote transmitido. Na outra extremidade o receptor separa cada fração do pacote e entrega ao canal respectivo.

A multiplexação TDM pode ser determinística ou estatística. Na determinística cada fração do pacote é exclusiva para cada canal, e se um canal deixar de transmitir esta parcela do pacote trafega vazia. O TDM estatístico pode aproveitar espaço vazio do pacote para transmitir outras informação (outros canais que estão transmitindo), teoricamente aproveitando o máximo a banda de transmissão. Este método, porém, exige a transmissão de informações adicionais, diminuindo o aproveitamento do meio de transmissão.

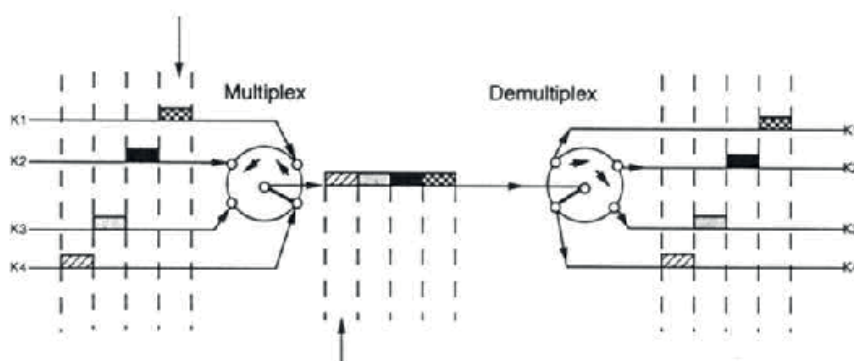



Figura 1.3.8: Multiplexação no tempo (TDM).

3.3.3 Multiplexação por divisão de código (CDM)

A multiplexação por divisão de código utiliza a ideia da codificação Spread Spectrum. O princípio é que uma vez codificado um sinal com uma determinada sequência, apenas essa mesma sequência é capaz de decodificar o sinal original. Assim, podemos enviar em um mesmo canal (frequência única) vários canais com diferentes códigos que são separados no destino.

Essa técnica possibilita uma maior densidade e capacidade de multiplexação. Por exemplo,um sistema CDM transmite três vezes mais que um sistema TDM semelhante, isto é, com mesma banda de transmissão. A maior desvantagem é a maior complexidade do sistema, produzindo um custo maior.

3.3.4 Multiplexação por comprimento de onda (WDM)

A multiplexação por comprimento de onda foi o início da revolução das redes óticas. Ela consiste em enviar através de uma única fibra ótica vários comprimentos de onda (lambda) que são separados no destino, mostrado na

Figura 1.3.9. Cada comprimento de onda transmite informações de um canal sem interferir nos demais. Isso é possível porque a banda útil de uma fibra ótica é muito maior que a necessidade de um canal.

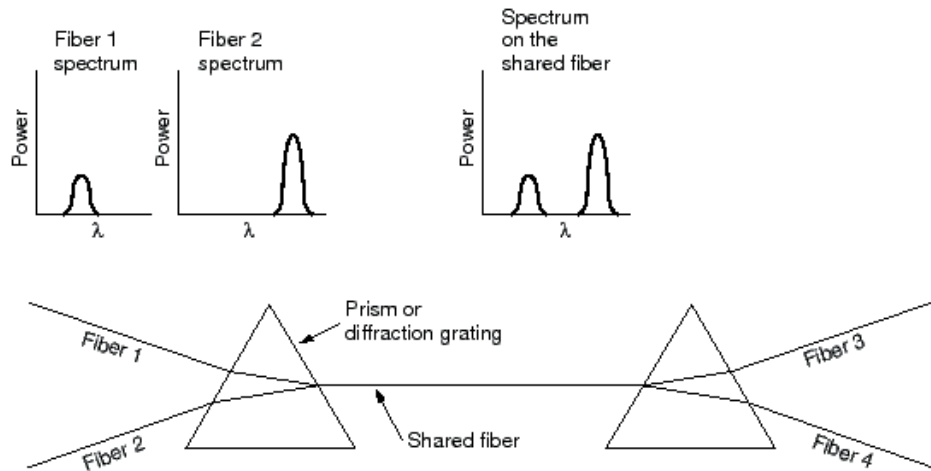
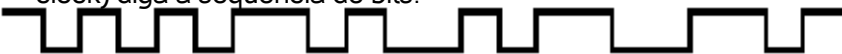



Figura 1.3.9: Multiplexação no comprimento de onda (WDM).

Como o comprimento de onda é igual à velocidade dividida pela frequência (λ = v/f) e como a velocidade de propagação é constante, podemos afirmar que a multiplexação pelo comprimento de onda é igual à multiplexação pela frequência. A diferença é que as frequências são muito grandes e fica mais confortável tratar os comprimentos de onda.

Atividades de avaliação

1. A transmissão Síncrona é mais eficiente que a transmissão Assíncrona? Caso positivo relacione as vantagens justificando cada uma delas.
2. Relacione as principais vantagens da codificação Manchester sobre a codificação NRZ.
3. Porque o código Manchester não deve ser utilizado em comunicações com taxas de transmissão muito altas.
4. A forma de onda a seguir representa uma codificação Manchester. Determine o início e fim de cada período de bit (isto é, extraia a informação de clock) diga a sequência de bits.

5. Como se chega ao valor de 64 KBPS usado em telefonia para a transmissão de voz em PCM.
6. Quais as vantagens da multiplexação TDM sobre a multiplexação FDM?

4. Interface

A camada física define as interfaces elétricas com os dispositivos de comunicação. A seção 4.1 apresenta os modems digitais e a seção 4.2 apresenta os modems analógicos e os esquemas de modulação. Finalmente a seção 4.3 mostra a interface RS-232 e a seção 4.4 a interface V.35.

4.1 Modem Digital Banda Base

4.1.1 Introdução

Os MODEMS BANDA BASE ou MODEMS DIGITAIS transformam o sinal digital em sinal digital codificado, para que este possa ser transmitido a maiores distâncias através do meio de comunicação.

Os circuitos utilizados são dedicados, ou seja, não utilizam os serviços da Rede Pública de Telefonia. Nos circuitos urbanos, utilizam LPCDs (Linhas Privativas de Comunicação de Dados) do tipo B (Banda de Base) e nos circuitos interurbanos são utilizados os modens analógicos.

O modem Banda Base é utilizado apenas em distâncias curtas (alguns quilômetros), pois a faixa de frequência disponível nos meios de comunicação é limitada (ocupam um espectro de frequência muito maior que 4 KHz, disponíveis em um canal de voz), devendo ser mantido em uma faixa de frequência com pouca DC (corrente contínua).

Outros aspectos importantes são:

- Utilizam como suporte de transmissão apenas par de fios, portanto não utilizam canal de rádio, multiplex etc.
- Devido as características dos sinais dos modems banda base, seu custo é muito menor que os modems analógicos.
- Não são padronizados pelo ITU-T, possuindo diversos tipos de codificação, de acordo com o fabricante.

4.1.2 Esquemas de Codificação

Podem ser usados os seguintes esquemas de codificação:

- Código NRZ
- Código Unipolar RZ
- Código Manchester ou Bifase
- Código de Miller
- Código AMI
- Código CMI
- Código HDB-3

4.1.3 Distância x Velocidade

A distância alcançada pelo modem banda base diminui conforme aumenta a velocidade de transmissão(bps). O alcance é definido como sendo a distância máxima em que ele consegue funcionar mantendo a taxa de erro abaixo de um valor predeterminado.

A relação distância (alcance) x velocidade de um modem banda base é mostrada na tabela 1.4.1.

Tabela 4.1:

RELAÇÃO DISTÂNCIA X VELOCIDADE MODEM BANDA BASE	
Distância (Km)	**Velocidade (bps)**
30	1200
18	2400
13	4800
9	9600
6	19200

A tecnologia Banda Base mais atual é chamada de xDSL. Com ela conseguimos atingir velocidades da ordem de MBPS em distância curtas (tipicamente até 3 Km). Pelo curto alcance também são chamados de dispositivo de última milha (last mille). Assim como os modens banda base, também não há padronização ITU-T, por isso um modem de um fabricante geralmente só pode comunicar com outro modem idêntico.

4.2 Modem Analógico para Rede Pública Telefônica Comutada

O sistema telefônico foi projetado e instalado com a finalidade de transportar a voz humana, sob forma de sinal elétrico, entre vários pontos. É basicamente composto pelos aparelhos telefônicos (terminais), as centrais de comutação (que permitem iterligar dois aparelhos) e as linhas telefônicas.

Esse sistema, que tem as características apropriadas para a transmissão do sinal de voz, tornou-se um meio atrativo para a transmissão de dados, pelo fato de já estar instalado numa extensão geográfica muito grande em quase todos os países.

4.2.1 A Linha Telefônica Comutada

A linha telefônica comutada é aquela fornecida pelas concessionárias do serviço telefônico, juntamente com o aparelho, em nossas residências e locais de trabalho. A extremidade desta linha é constituída por dois fios e ela é responsável por ligar os aparelhos telefônicos à central telefônica mais próxima, com a qual mantém-se o primeiro contato.

4.2.2 Modens V22 e V22bis

Os modelos de modens V22 e V22bis operam full-duplex em dois fios. O modem V22 utiliza a modulação DPSK (Differential Phase Shift Keying) e o modem V22bis utiliza a modulação QAM (Quadrature Amplitude Modulation).

A transmissão destes modens é sempre síncrona e eles utilizam a multiplexação por divisão de frequência (FDM) para conseguir a comunicação duplex em apenas dois fios, de forma semelhante ao modem tipo V21. A comunicação assíncrona é conseguida devido a um circuito conversor síncrono/assíncrono que faz parte integrante desses modens.

A Recomendação V22

Um modem V22 é um modem "síncrono/assíncromo" que provê uma operação a 1200 bps full-duplex em um circuito de dois fios. Ele executa a multiplexação por divisão de frequência para criar dois sub-canais na largura de banda de uma linha de dois fios; um canal é usado para enviar e outro para receber dados.

Este modem pode transmitir em cinco modos diferentes, sendo dois síncronos e três assíncronos, com relação ao ETD. Com relação à linha telefônica, sua transmissão é sempre síncrona.

Os modos assíncronos são chamados de modos start-stop e possuem uma concepção diferente dos modens FSK: um conversor "síncrono/assíncrono" faz a transformação dos dados assíncronos provenientes do ETD para a forma síncrona a ser efetivamente transmitida.

A Recomendação V22bis

Modens V22bis transmitem full-duplex a dois fios, para uso na rede telefônica pública, com sua velocidade limitada em 2400 bps. Estes modens usam FDM assim como os modens modelos V22. Quando estão operando a 2400 bps usam a modulação QAM e quando operam a 1200 bps usam DPSK também como os V22.

Os modens V22bis podem transmitir em quatro modos diferentes, sendo dois síncronos e dois assíncronos. De maneira similar ao modem V22, sua transmissão na linha telefônica é sempre síncrona. A tabela 1.4.2 mostra os quatro modos de transmissão do modem V22bis:

Tabela 4.2:

MODOS DE TRANSMISSÃO MODEM V22BIS				
Modo	Velocidade[bps]	Tolerância	Taxa[baud]	Bits por caractere
1	2400 sinc	0,01%	600	-
2	2400 assi	+1% -2,5%	600	8 a 11
3	1200 sinc	0,01%	600	-
4	1200 assi	+1% -2,5%	600	8 a 11

Nas transmissões a 2400 bps os dados são agrupados em símbolos com quatro bits consecutivos. Os dois primeiros bits (Q1 e Q2) definem a variação diferencial de fase e os dois últimos definem a posição relativa dentro do quadrante. Os bits Q1 e Q2 passam por um conversor e pelo integrador módulo 4, cuja saída, juntamente com os bits Q3 e Q4, alimenta o gerador de quadratura.

O Modulador QAM

Um modem QAM consegue transmitir o máximo de dados sobre uma linha analógica. A Figura 1.4.1 mostra um exemplo de codificação QAM de um modem V22bis e V32 respectivamente.

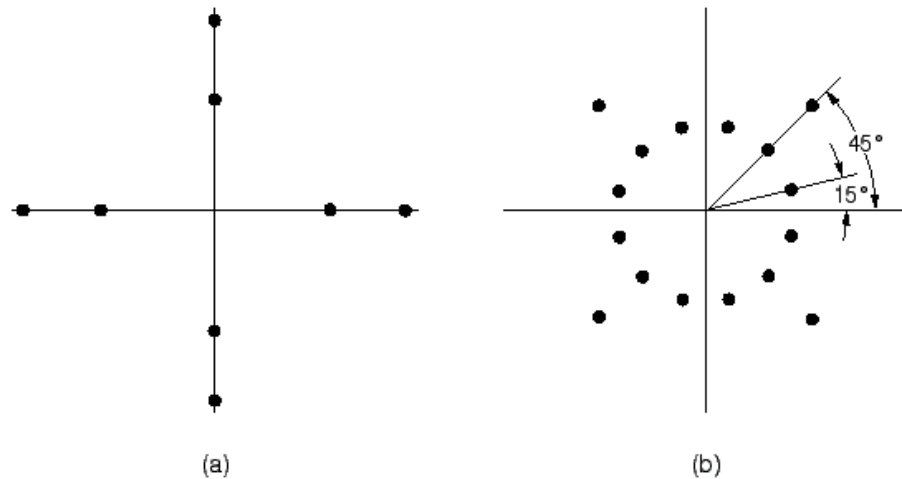



Figura 1.4.1: Modulação QAM V22bis e V32.

O modulador QAM tem a função de modular uma portadora senoidal, cuja frequência vai depender do modo de operação do modem (O/R = origem/resposta). A tabela 1.4.3 mostra os valores.

Tabela 1.4.3:

ESPECIFICAÇÃO MODULADOR DPSK E QAM DOS MODENS V22, V22BIS E V32				
Modem	**Portadora O.**	**Portadora R.**	**Modulador**	**Símbolos**
V22	1200 Hz	2400 Hz	DPSK	4 (1200 bps)
V22bis	1200 Hz	2400 Hz	QAM	8 (2400 bps)
V32	1200 Hz	2400 Hz	QAM	16 (9600 bps)

O espectro de transmissão é exatamente o mesmo para esses dois tipos de modens. Quando o modem local opera no modo origem ele utiliza o canal mais baixo para transmitir e recebe pelo canal mais alto enquanto o modem remoto deve estar operando no modo resposta de forma inversa.

Um tom de guarda na frequência de 1800 Hz (+/-) 20 Hz pode ser transmitido simultaneamente com o sinal principal se este estiver ocupando o canal alto. O tom de guarda pode ser, opcionalmente, na frequência de 550 Hz (+/-) 20 Hz.

4.3 Interface RS-232

4.3.1 Introdução

No mundo da comunicação de dados, os equipamentos como computadores pessoais, terminais e portas de computador são chamados de Equipamentos Terminais de Dados (ETDs). Por outro lado, modems e outros dispositivos de comunicação são conhecidos como Equipamentos de Comunicação de Dados (ECDs).

A interface digital é um dispositivo de entrada e saída que torna possível a compatibilidade entre um ETD e um ECD.

A compatibilidade é obtida pela padronização a nível internacional da interface. A primeira tentativa de padronização ocorreu em 1969, quando os fabricantes de equipamentos, o laboratório BELL e a EIA (Eletronic Industries Association) especificaram a RS-232, que logo em seguida com algumas alterações, tornou-se o padrão RS-232 C. Paralelamente, o CCITT (Comité Consultatif Internacional Telegraphique et Telephonique), hoje ITU (International Telecommunication Union), também padronizou a interface terminal-modem, através das Recomendações V.24/V.28, compatível com a RS-232 C.

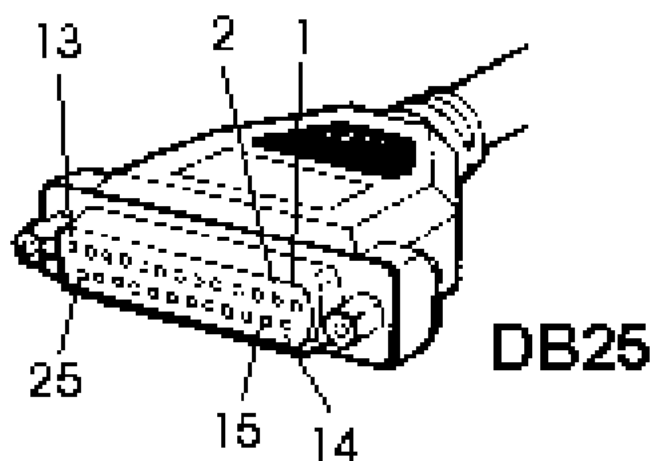



Figura 1.4.2: Conector DB-25 RS-232/V.24.

A interface mecânica é padronizada pela ISO (International Organization for Standartization) através da norma ISO 2593-1973, compatível com a CCITT V.24, utilizando um conector DB-25. A Figura 1.4.2 mostra um conec-

tor com a identificação dos pinos. No Brasil, os modems devem atender ao Padrão Telebrás 225-540-730 de 1986, baseado nas normas EIA RS-232 C, CCITT V.28 e CCITT V.24.

4.3.2 Evolução dos Padrões de Interface

Com a finalidade de normalizar as facilidades de comunicação em todo o mundo, foram criados alguns órgãos para desenvolvimento de padrões comuns associados aos serviços de telefonia internacional.

Dentre os padrões de interface, o CCITT V.24/V.28 e o EIA RS-232 C são os mais conhecidos. No item Recomendações CCITT é apresentado um resumo das recomendações que constam no Yellow Book da CCITT.

A EIA é um órgão que representa grande parte dos fabricantes da indústria de equipamentos eletrônicos dos Estados Unidos. O trabalho da EIA na normalização é altamente reconhecido, e muitos dos seus padrões e normas foram adotados por outros órgãos especializados no assunto.

O RS-232C é um padrão recomendado, publicado pela EIA em 1969. O número 232 representa o número de identificação de um determinado padrão de comunicação, e o sufixo C designa a última revisão feita a esse padrão.

O padrão RS-232C e os padrões estabelecidos pelas normas CCITT V.24 e V.28, são muito semelhantes, e diferem basicamente apenas na nomenclatura da pinagem da interface.

No final do anos 70, a EIA pretendeu substituir gradativamente o padrão RS-232 C por um conjunto de três padrões: o RS-449, o RS-422 e o RS-423. Eles foram projetados não só para permitir taxas de transmissão de dados mais altas que as obtidas com o RS-232 C, como também para proporcionar uma maior funcionalidade. Embora a EIA e vários outros órgãos governamentais tenham firmemente promovido o padrão RS-449, sua adoção pelos fabricantes tem sido limitada. Reconhecendo o fato de que a adoção universal do RS-449 e seus padrões associados era basicamente impossível, a EIA produziu o RS-232 D (revisão D) em janeiro de 1987 e um novo padrão conhecido como RS-530.

As maiores diferenças entre o RS-232 D e o RS-232 C são as seguintes:

- A nova revisão aceita operações de teste para os equipamentos de comunicação remota e local através do uso de sinais compatíveis com essa função.
- A nova revisão modifica o uso do condutor Protective Ground (Terra de proteção, pino 1 da interface) para fornecer uma forma de blindagem.
- Geralmente, os dispositivos criados para os padrões RS-232 C e RS-232 D, são compatíveis com os dispositivos criados para os padrões CCITT V.24/V.28.

4.3.3 Pinagem do padrão EIA RS-232/CCITT V.24

A diferença básica entre o padrão CCITT V.24 e o padrão EIA RS-232 consiste apenas na designação da pinagem do conector DB-25. A tabela 1.4.4 apresenta:

- os pinos do conector DB-25
- a nomenclatura EIA RS-232-C para idetificação do circuito
- a nomenclatura CCITT V-24
- a fonte do sinal
- a abreviatura da descrição da função do circuito
- a descrição da função do circuito

Tabela 1.4.4:

PINAGEM RS-232/V.24					
PINO	**RS-232**	**V.24**	**FONTE**	**ABREV.**	**DESCRIÇÃO**
1	AA	101	AMBOS	PG	Protective Ground
2	BA	103	ETD	TD	Transmitted Data
3	BB	104	ECD	RD	Received Data
4	CA	105	ETD	RTS	Request to Send
5	CB	106	ECD	CTS	Clear to Send
6	CC	107	ECD	DSR	Data Set Ready
7	AB	102	AMBOS	SG	Signal Ground
8	CF	109	ECD	CD	Carrier Detect
9	-	-	-	-	Reservado para teste do modem
10	-	-	-	-	Reservado para teste do modem
11	-	-	-	-	Livre
12	SCF	122	ECD	SCD	Sec. Rec.Signal Detect
13	SCB	121	ECD	SCT	Sec. Clear to Send
14	SBA	118	ETD	STD	Sec. Transmitted Data
15	DB	114	ECD	ST	Transmit Timing
16	SBB	119	ECD	SRD	Sec. Received Data
17	DD	115	ECD	RT	Received Timing
18	-	-	-	-	Livre
19	SCA	120	ETD	SRT	Sec. Request to Send
20	CD	108.2	ETD	DTR	Data Terminal Ready
21	CG	110	Qualquer	SQD	Signal Quality Detector
22	CE	125	ECD	RI	Ring Indicator
23	CH/CI	111	Qualquer	DRD	Data Rate Detector
24	DA	113	ETD	ST	Transmit Timing
25	-	-	-	-	Livre

4.3.4 Sinais de Controle de Transmissão

Os sinais nos pinos 4 (RTS), 5 (CTS), 6 (DSR) e 20 (DTR) são chamados Sinais de Controle de Transmissão, pois controlam a sequência de ações necessárias para que os modens aceitem dados dos terminais e façam a modulação. Eles também possibilitam a comunicação entre dois modens.

Abaixo mostramos a sequência operacional dos sinais de controle. Quando o modem é ligado, as seguintes ações ocorrem:

1. O modem passa um sinal DSR (Data Set Ready) para o terminal.
2. Ao receber uma chamada, o modem responde à voltagem do sinal de toque de chamada ativando/desativando o pino 22 (Ring Indicator). Alguns terminais emitem o DTR (Data Terminal Ready) assim que são ligados, outros emitem este sinal em resposta a um sinal Ring Indicator.
3. O modem transmissor emite um tom de onda portadora para o modem receptor. A recepção desse tom indica a continuidade do circuito estabelecido por um modem tentando se comunicar com outro através da rede telefônica pública e o fato de que há um modem na outra extremidade do circuito. Caso não receba o tom de onda portadora, o modem não ativa o pino 8 (Carrier Detect) para seu respectivo ETD, e a ligação cai.
4. Se o ETD for um computador, a confirmação de um sinal Ring Indicator seguido de um sinal Carrier Detect indica que a ligação foi adequadamente estabelecida e que a transmissão pode iniciar.
5. Normalmente o computador transmite algum tipo de mensagem de "boas vindas" para o dispositivo remoto que está tentando acessá-lo.
6. Para transmitir dados, o computador emite seu sinal RTS (Request to Send) , que deve ser reconhecido pelo modem. O modem emite seu controle CTS (Clear to Send), que indica que ele recebeu um tom de onda portadora e está pronto para modular dados.
7. Nesse momento, a porta do computador transmitirá dados para o pino2 do modem (Transmitted Data) e receberá dados modulados no pino 3 (Received Data).

4.3.5 Características de Sinal da RS-232

A Interface RS-232 especifica 25 circuitos de ligação, ou condutores, que controlam o fluxo de dados entre o ETD e ECD. O sinal de cada um desses condutores ocorre de acordo com uma transição de voltagem predefinida.

Dessa forma, os padrões estabelecem os níveis de tensão para a transmissão de dados, onde o estado lógico 1 (marca) é definido como sendo uma tensão negativa entre -3 e -15 volts, enquanto o estado lógico 0 (espaço) é definido como uma tensão positiva entre +3 volts e +15 volts, tudo referenciado ao terra de sinal e com previsão de uma queda de tensão de 12 volts ao longo das linhas de transmissão.

Como os receptores são obrigados a reconhecer sinais de no máximo +-3 volts, sobra uma margem de segurança (região de transição) de 6 volts

entre os níveis 1 e 0, o que contribui para aumentar a imunidade a ruídos e a diferença de potencial de massa. O estado do sinal não necessariamente será identificado de forma única quando a tensão estiver na região de transição.

Sob o RS-232-D, as faixas de voltagem ON e OFF foram estendidas para +25V e -25V, respectivamente. A tabela 4.5 compara a voltagem do circuito de ligação, seu estado binário, condição de sinal e função.

Tabela 1.4.5

SINAL ELÉTRICO DA INTERFACE RS-232			
Voltagem circ. Lig	**Positiva**	**Negativa**	**Indefinido**
TENSÃO	+3 e +15V	-3 e -15V	-3 e +3V
ESTADO BINÁRIO	0	1	x
CONDIÇÃO DO SINAL	Espaço	Marca	x
FUNÇÃO	ON	OFF	x

A norma RS-232 recomenda o uso de cabos curtos, com comprimento de até 15 metros, embora ressalte que cabos mais longos são permitidos, desde que resultem numa capacitância de carga inferior a 2,5 nF.

4.3.6 Ligação Cross-Over

Quando deseja-se ligar dois equipamentos de mesmo tipo (terminal-terminal, modem-modem) pelo seu lado digital, deve-se utilizar o cabo Cross-Over mostrado na Figura 1.4.4. Este cabo faz a inversão (cruzamento) entre os sinais.

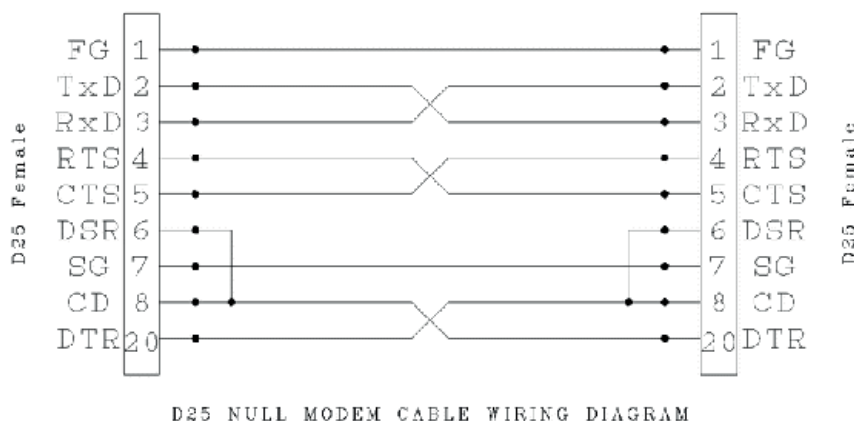



Figura 1.4.4: Cabo RS-232 DB-25 Cross-Over (Null-modem).

A interligação dos pinos da interface pelo cabo Cross-Over é a seguinte:

- Os pinos 1 e 7 são terra que precisa ser igual em ambos os lados, o pino 1 refere-se ao terra do chassi e o pino 7 o terra do sinal.

- O cruzamento dos pinos 2 e 3 é necessário, pois o que é transmissão num dispositivo é recepção no outro, e vice-versa;
- Os pinos 4 e 5 são cruzados, pois os sinais RTS/CTS indicam a requisição e autorização para transmissão.
- O pino 20 (DTR) do primeiro terminal é ligado ao pino 8 (CD) e pino 6 (DSR) do outro terminal. O sinal DTR indica que o terminal está pronto para transmitir que indicará ao outro terminal que a conexão está estabelecida. Faz-se a mesma ligação no sentido inverso do outro terminal para o primeiro terminal.

4.4 Interface V.35

4.4.1 Introdução

A recomendação V.35 da CCITT estabelece a transmissão de dados a partir de 48 kbits/s usando largura de banda na faixa de 60 a 108 kHz.

Preferencialmente esta transmissão deverá ser no modo síncrono, operando em modo full-duplex e utilizando modulação em amplitude.

4.4.2 Descrição da Interface V.35

Segundo as normas da CCITT a interface V.35 é composta pelos circuitos mostrados na tabela 1.4.6.

Tabela 1.4.6

SINAIS DA INTERFACE V.35	
Número	**Descrição**
102	Signal Graund (SG) ou common return (Terra de Sinalização)
103	Transmitted Data (TD) (Dados Transmitidos)
104	Received Data (RD) (Dados Recebidos)
105	Request to Send (RTS) (Solicitação para Envio)
106	Clear to Send (CTS) (Inicialização para Envio)
107	Data Set Ready (DSR) (Conjunto de Dados Pronto)
109	Carrier Detect (CD) (Detecção de Portadora)
114	Transmitter Signal Timing (Temporizador do Sinal de Transmissão)
115	Receiver Signal Timing (Temporizador do Sinal de Recepção)

Mostramos a seguir o detalhamento de cada sinal de controle.

102 / Signal Graund(SG) or common return (Terra de Sinalização)

Estabelece uma referência de aterramento para todas as linhas, incluindo dados, temporização e sinais de controle. A voltagem nesse circuito é definida como 0V para que haja uma referência para todos os sinais.

103 / Transmitted data (TD) (Dados Transmitidos)

Este é o circuito através do qual o fluxo serial de bits de dados passa do terminal para o modem, onde é modulado para transmissão.

104 / Received Data (RD) (Dados Recebidos)

Depois que um modem demodula os dados, eles são transferidos para o terminal através desse circuito ligação. Quando o modem não está enviando dados para o terminal, esse circuito fica na condição de marcação.

105 / Request to Send (RTS) (Solicitação para Envio)

O sinal desse cirucito é enviado pelo terminal (DTE) ao modem para prepará-lo para a transmissão de dados. Antes de enviar os dados, o terminal deve receber um sinal Clear to Send do modem.

106 / Clear to Send (CTS) (Inicialização para Envio)

Esse circuito de ligação envia um sinal ao terminal indicando que o modem está pronto para transmitir. Desligando esse circuito, o modem informa ao terminal que não está pronto para receber dados. O modem emite o sinal CTS depois que terminal inicializa um sinal Request to Send (RTS).

107 / Data Set Ready (DSR) (Conjunto de Dados Pronto)

Os sinais nesse circuito de ligação indicam o status do modem conectado ao terminal. Quando esse circuito está ativo (ON - nível lógico 0), ele serve como um sinal para informar ao terminal que o modem está conectado à linha telefônica e está pronto para transmitir dados.

109 / Carrier Detect (CD) (Detecção de Portadora)

Um sinal nesse circuito indica ao terminal que o modem está recebendo um sinal de onda portadora de um modem remoto.

114 / Transmitter Signal Timing (Temporizador do Sinal de Transmissão)

Utilizado quando o DCE fornece o sinal de temporização.

115 / Receiver Signal Timing (Temporizador do Sinal de Recepção)

Utilizado quando o DCE recebe o sinal de sincronização através da linha a qual ele está conectado.

Atividades de avaliação

1. Descreva as funções de uma interface.
2. Observando a Tabela 4.1 observamos que quanto maior a distância menor a taxa de transmissão. Depois de ler a seção que fala sobre dificuldades de transmissão, explique porque isso ocorre.
3. Por que é necessário modular um sinal para transmitir por longa distâncias?

Síntese do capítulo

Neste capítulo apresentamos os conceitos básicos de Redes de Computadores. Iniciamos com uma introdução com a história da Internet e a definição de alguns conceitos que serão necessários para o entendimento das unidades e capítulos seguintes. Depois apresentamos os princípios da transmissão de dados e a codificação de dados mostrando os problemas do mundo real para transmitir uma informação e as maneiras para contorná-la. Finalmente apresentamos as principais interfaces de comunicação de dados começando pelas mais antigas até as mais modernas.

Leituras, filmes e sites

Filmes

A Rede Social (The Social Network) é um filme norte-americano lançado em 2010 que é um drama sobre a fundação do website Facebook. O filme foi dirigido por David Fincher e possui em seu elenco os atores, Andrew Garfield, Justin Timberlake, Armie Hammer e Max Minghella. Esse filme não recebeu a aprovação dos fundadores do Facebook mas é uma boa diversão e mostra bem o mundo dos negócios na Internet.

Sites

Página da Wikipedia com vasto material sobre Redes de Computadores (em português)

http://pt.wikipedia.org/wiki/Rede_de_computadores

A história da Internet contada pelos seus criadores (em inglês)

http://www.isoc.org/internet/history/brief.shtml

A história da Internet contada pelos seus criadores (em português, tradução não oficial)

http://www.aisa.com.br/historia.html

Referências

ANDREW S. TANENBAUM **Redes de Computadores** 4ª Ed. Editora: Campus, 2004. Livro de referência clássica com mais de 30 anos desde a primeira edição, proporcionando ao estudante uma visão histórica das arquitetura e protocolos de redes de computadores. São quase 1.000 páginas de texto com descrição detalhada dos sistemas e protocolos, além disso, o autor tem um ótimo senso de humor tornando a leitura muito agradável.

Shimonski, Steiner e Sheedy **Cabeamento de Rede** Editora: LTC, 2010. Livro específico sobre cabeamentos de redes par trançado, coaxial e fibra ótica. O livro inicia com uma ótima fundamentação teórica sobre transmissão de sinais e os problemas de interferência. Discute as normas de cabeamento e os cuidados com interferência elétrica. O texto apresenta também aspectos práticos de instalação de cabeamento e utilização de ferramentas.

WILLIAM STALLINGS. **Redes e Sistemas de Comunicação de Dados.** 1ª Ed. Editora: Campus, 2005. Este livro trata dos fundamentos de comunicação de dados sob a ótica de gerenciamento de negócios e de informação. Apresenta uma visão menos técnica e mais gerencial, por isso é um ótimo complemento a outros livros de redes.

Capítulo 2

Arquitetura de Protocolos de Comunicação

Objetivos

- Nesta unidade vamos apresentar as arquitetura de vários protocolos de comunicação usados em Redes de Computadores. Iniciamos com conceitos gerais de uma camada de Enlace genérica com seus princípios. Depois apresentamos detalhes da camada de enlace com vários exemplos de protocolos para redes de longa distância (WAN), redes locais (LAN) e, finalmente, redes locais sem fio (WLAN).

1. Enlace

O envio de sinais por um meio físico não é suficiente para estabelecer uma comunicação entre dois pontos. A camada de enlace é responsável em estabelecer, manter e liberar conexões entre entidades de rede; transferir unidades de dados de serviço de enlace com rapidez, flexibilidade e economia; detectar e corrigir os erros provenientes do nível físico. A seção 5.1 apresenta as características e funcionalidades da camada de enlace, a seção 5.2 apresenta o enquadramento de um quadro na camada de enlace, a seção 5.3 mostra alguns mecanismos para controle de fluxo, a seção 5.4 apresenta as técnicas para detecção de erro e, finalmente, a seção 5.5 os mecanismos para correção de erros.

1.1 Funções da camada de Enlace

O nível de enlace é responsável em estabelecer, manter e liberar conexões entre entidades de rede; transferir unidades de dados de serviço de enlace com rapidez, flexibilidade e economia; detectar e corrigir os erros provenientes do nível físico.

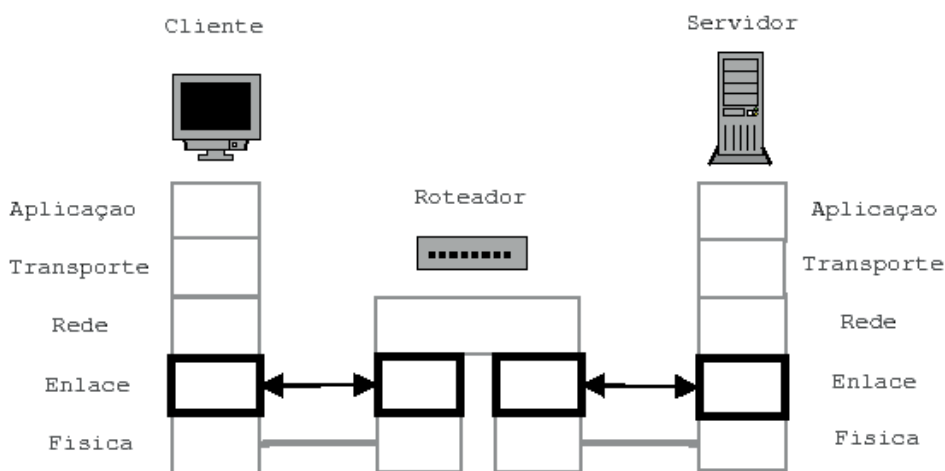



Figura 2.1.1: Diagrama da camada de Enlace.

A camada de Enlace fica entre a camada Física e Rede. Ela trata de ligações ponto a ponto, apenas entre dois equipamentos (ou vários no mesmo meio físico, se for rede local). A camada de enlace não sabe decidir o que fazer se a mensagem não pertence a um deles, função esta exercida pela camada de rede. A Figura 2.1.1 mostra esquematicamente o diagrama da camada de enlace.

As principais funções do nível de enlace são:

- Enquadramento
- Controle de Fluxo
- Controle de Erro

Quando a conexão dos pontos é realizada somente a nível local, algumas características de comunicação são diferentes das utilizadas em conexões de longa distância. São elas:

- Transmissão em velocidades maiores, mesmo que o meio de transmissão seja simples (par metálico);
- Meios de transmissão que apresentam menor taxas de erros (cabo coaxial, fibra ótica);
- Acesso direto ao meio, podendo utilizar as seguintes topologias: estrela, barra e anel.

Em vista das características acima citadas, o modelo OSI foi adaptado para referenciar também as redes locais: a camada de enlace foi subdividida em duas camadas:

- LLC. Responsável em implementar a interface do nível de enlace com o nível de rede, fornecer serviços como multiplexação e o controle do fluxo e dos erros.
- MAC. Responsável em manipular as características específicas das várias tecnologias de redes locais, isto é, responsável pelo acesso ao meio.

A camada de enlace foi subdividida com a finalidade de possuir um nível independente da topologia, dos meios de transmissão e dos métodos de acesso utilizados na rede local, de forma que, se alterações fossem realizadas nestes itens, o protocolo de enlace não seria alterado. Esse nível é o LLC.

1.2 Enquadramento

A camada de enlace é a primeira onde os dados são montados, pois a camada inferior trata apenas das interfaces físicas. A primeira função da camada de enlace é o enquadramento que consiste em delimitar o início e fim do quadro de mensagens e incluir caracteres de controle. A relação das funções de enquadramento são mostradas abaixo:

1. Delimitator de início e fim de quadro.
2. Contagem de caracteres.
3. Preenchimento de caractere ou bit.
4. Violações de enquadramento.

Ao receber um quadro, devemos verificar se ele já chegou completo e se algum dado foi perdido. Para isso incluímos um caractere especial que define o início e o fim do quadro, no qual chamamos flag.

Apenas essa informação não é suficiente para garantir uma mensagem completa, pois poderá haver um erro no bit de um caractere que se transforma em caractere de fim, terminando a mensagem prematuramente. Assim, um campo do quadro oferece o tamanho total do quadro, permitindo ao receptor receber a mensagem completa e verificar se houve algum erro na transmissão.

A utilização de caractere de início e fim de quadro impõe a limitação não podermos transmitir esse caractere no meio da mensagem pois o receptor pode interpretá-lo como fim da mensagem. Para evitar esse problema é utilizada a técnica de preenchimento de bit (bit stuffing). Por exemplo, toda vez que for encontrado uma sequência de bits igual ao flag “011111xx”, o enlace insere automaticamente um “0”, transformando a sequência em “0111110xx”, evitando uma sequência correspondente ao flag. Na recepção, toda vez que for encontrada uma sequência “0111110xx” o “0” é descartado antes do dado ser processado, refazendo a sequência original. Se ocorrer a sequência “0111110”, esta será identificada unicamente como um flag. Não existe risco de confundir a nova sequência com outro caractere, pois o “0” sempre é retirado no receptor após encontrar a sequência “0111110xx” restaurando o caractere original. Um exemplo de preenchimento de bit é mostrado na Figura 5.2.

(c) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

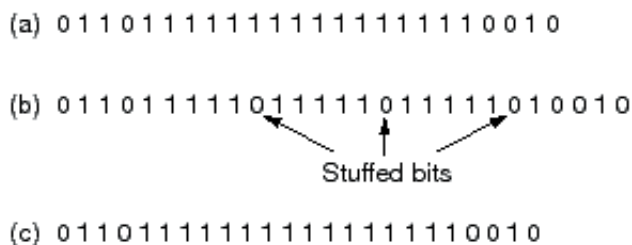



Figura 2.1.2: Preeenchimento de bit.

Outra função importante é a verificação do enquadramento. Essa função consiste em verificar a correta formação do quadro, isto é, se os caracteres de controle existem e se as informações estão colocadas na posição correta do quadro.

1.3 Controle de fluxo

Chamamos controle de fluxo ao processo de cadenciamento da transmissão de uma sequência de pacotes enviados do transmissor para o receptor. Este controle é importante porque devemos enviar a mensagem (conjunto de pacotes) o mais rápido possível, mas devemos enviar o suficiente para que o receptor possa recebê-los sem perdas.

Mas como saber se o receptor está recebendo perfeitamente? O recebimento das confirmações do receptor cadencia a transmissão pelo transmissor.

1.3.1 Controle de fluxo Para-e-Espera (Stop-and-Wait)

O controle de fluxo mais simples é chamado para-e-espera (stop-and-wait). Neste caso o transmissor envia um pacote e fica aguardando a chegada da confirmação, quando então pode enviar outro pacote. Se não receber a confirmação em um certo período considera que o receptor não recebeu o pacote, por isso retransmite o pacote novamente esperando pela confirmação.

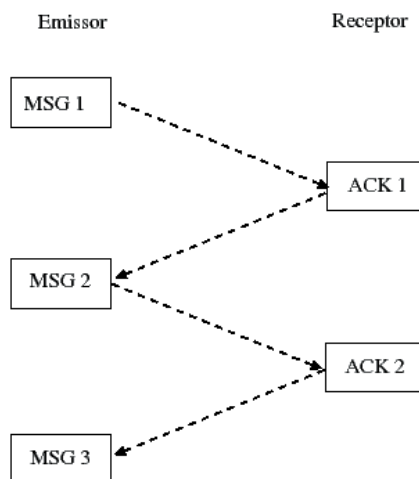



Figura 2.1.3: Funcionamento do mecanismo para-e-espera.

1.3.2 Controle de fluxo por Janelas Deslizante (Sliding-Window)

O controle stop-and-wait é simples e eficiente e foi utilizado durante muito tempo como controle de fluxo dos protocolos mais antigos, por exemplo, BSC-3. Se a linha de comunicação é muito longa (latência alta), como comunicação via satélite, ou quando a rede é muito veloz, ocorre um fenômeno chamado memória da rede. Isso se refere a quantidade de pacotes que estão viajando antes de chegar o reconhecimento.

Uma solução para este problema foi enviar mais pacotes antes de receber o reconhecimento do primeiro pacote. Com isso podemos encher a linha

de comunicação e aproveitar mais a capacidade. Esse mecanismo se parece com uma janela deslizante, por isso foi denominado assim (sliding-window). Como agora temos vários pacotes viajando precisamos identificar qual já chegou, por isso, os protocolos que implementam a janela deslizante tem um número de sequência no cabeçalho. Para permitir adaptação do mecanismo é possível variar o tamanho da janela durante a transmissão, ajustando a quantidade de pacotes de acordo com a condição da rede.

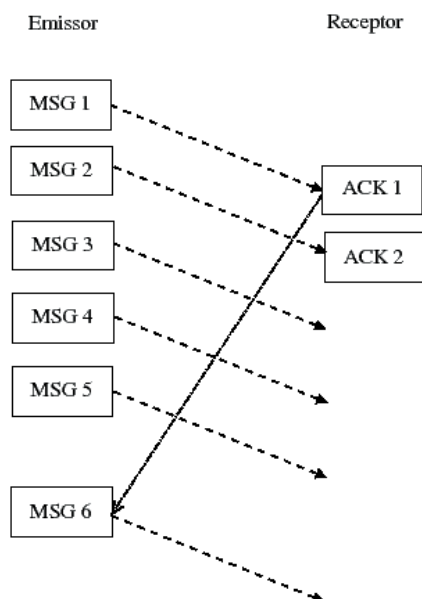



Figura 2.1.4: Funcionamento do mecanismo de janela deslizante.

A Figura 2.1.4 mostra um transmissor começa a transmitir uma mensagem. Inicialmente consideramos uma janela de cinco pacotes. Assim ele transmite 5 mensagens e fica aguardando a confirmação do primeiro pacote. Quando ela chega ao transmissor este pode enviar mais um pacote, para manter a janela de 5. Se receber todas as 5 confirmações sem retransmissão o transmissor pode aumentar a janela, por exemplo para 6. Se houver alguma perda de pacote ou confirmação o transmissor pode diminuir a janela, por exemplo para 3. Esse mecanismo de ajuste do tamanho da janela é chamado slow-start. O protocolo TCP é um exemplo que utiliza o mecanismo de janela deslizante.

1.4 Detecção de Erros

A detecção de erro é um método de se incluir um código que segue junto à mensagem e possibilita que o receptor verifique se a mensagem está integra, idêntica à mensagem transmitida. O diagrama mostrado na Figura 2.1.5 mostra o funcionamento da detecção de erro.

O transmissor calcula um número em função dos dados que vai transmitir. O transmissor inclui esse número ao final da mensagem e transmite. O receptor lê a mensagem e separa o número dos dados. O receptor calcula o número baseado na mensagem recebida. Se o número calculado for igual ao número recebido a mensagem está íntegra, senão a mensagem apresenta algum erro.

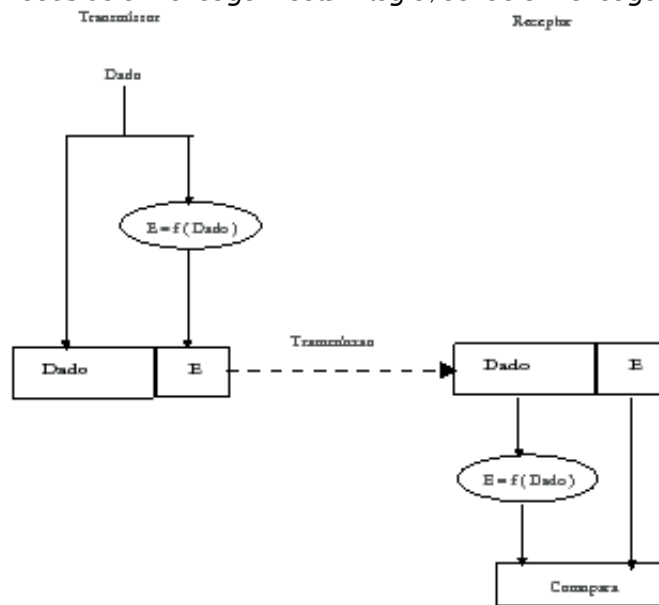



Figura 2.1.5: o funcionamento da detecção de erro.

1.4.1 Códigos de Detecção de Erros

Um conceito importante para determinar códigos de correção e detecção de erros é o da distância de Hamming. Existem diversos tipos de códigos, alguns mais indicados para tratamento serial, outros para paralelo. Algumas palavras de código são construídas concatenando ao final dos bits de informação o código correspondente, estes códigos são ditos separáveis, como é o caso dos códigos de paridade. Nos códigos não-separáveis, a palavra de código é obtida com o entrelaçamento do código com a informação, o código em m--entre-n é um exemplo de código não-separável.

Um dos códigos mais conhecidos e utilizados é o de paridade e o código aritmético. Embora os códigos de paridade sejam muito utilizados para a transmissão e armazenamento de dados, eles não são preservados por operações aritméticas.

Outro código bastante conhecido é o checksum que também faz parte dos separáveis.

Um código cíclico é definido pelo seu polinômio gerador G(x), que possui um grau (n–k). Dois códigos cíclicos conhecidos para detecção de erros são o CRC-12, CRC-16 e CRC-CCITT.

Distância de Hamming

A distância Hamming é determinada pelo número de bits diferentes em duas palavras. Assim, em um subconjunto S que contenha palavras de código com distância 2, uma transição para distância 1 pode representar uma palavra de código com erro de um bit.

1.4.2 Paridade

No código de paridade um bit é concatenado a informação, fazendo com que a palavra de código possua um número ímpar de bits 1 (paridade ímpar), ou um número par de bits 1 (paridade par). Esse código é utilizado no tratamento serial de informações, com detecção on-line de erros, sendo de fácil implementação.

1.4.3 Checksum

O checksum é utilizado em comunicação de dados e armazenamento sequencial. A palavra de código é formada por todas as palavras de informação concatenadas com um código gerado pela soma dessas palavras. Este código apresenta três desvantagens, a primeira é que o código funciona bem apenas com blocos contendo bastante quantidade de informação. Outra desvantagem é o fato da detecção não ser on-line, pois todas as palavras do bloco tem que ser lidas para calcular o checksum, e o tempo de detecção será o mesmo para um erro na primeira palavra ou na última. A terceira desvantagem é quanto a dificuldade de diagnóstico do erro, que em memórias pode ocorrer no bloco de palavras, no checksum armazenado ou no circuito de verificação. Na transmissão de dados, o erro pode estar na fonte dos dados, no meio de comunicação ou no circuito de verificação.

Um exemplo de uso de checksum é nos arquivos no formato hexadecimal gerados pelos compiladores para uso em processadores da Intel.

1.4.4 Cyclic Redundancy Check (CRC)

O CRC é um código de redundância polinomial muito usado e mostrados a seguir. O CRC-12, mostrado na equação 5.1, possui um total de 12+ k bits, sendo que k são de informação (12+ k, k). Da mesma maneira o CRC-16, mostrado na equação 5.2, e CRC-CCITT, mostrado na equação 5.3, pode ser definido por (16+ k, k). Além desses também é comum o código CRC-32, mostrado na equação 5.4.

$$CRC-12 = x^{12} + x^{11} + x^3 + x^2 + x^1 + 1 \quad (5.1)$$

$$CRC-16 = x^{16} + x^{15} + x^2 + 1 \quad (5.2)$$

$$CRC-CCITT = x^{16} + x^{12} + x^5 + 1 \quad (5.3)$$

$$CRC-32 = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{10} + x^8 + x^7 + x + 1 \quad (5.4)$$

O CRC-12 é utilizado para caracteres de 6 bits enquanto os outros são usados para caracteres de 8 bits. O CRC-16 e CRC-CCITT pode detectar todos os erros simples e duplos, todos os números ímpar de erros, todos os erros de rajadas menores que 16 bits e 99,998% dos erros de rajada de mais de 17 bits.

Um exemplo de cálculo de um polinômio CRC para o byte 1101011011 é mostrado na Figura 2.1.6. O funcionamento é bem simples, inicialmente os registradores do polinômio gerador (CRC) são preenchidos com algum valor, como por exemplo zero. Os bits de informação são transmitidos serialmente, cada um provocando uma alteração na primeira porta XOR, que iniciará um deslocamento pelo restante do circuito. Após toda a palavra ter sido transmitida, o CRC estará pronto, sendo também transmitido. Na recepção existe um G(X) idêntico preenchido com os mesmos valores iniciais. Após a recepção da informação ambos G(X) devem conter o mesmo valor de CRC, e finalmente após a recepção, o CRC do receptor deve conter seu valor inicial, por exemplo zero.

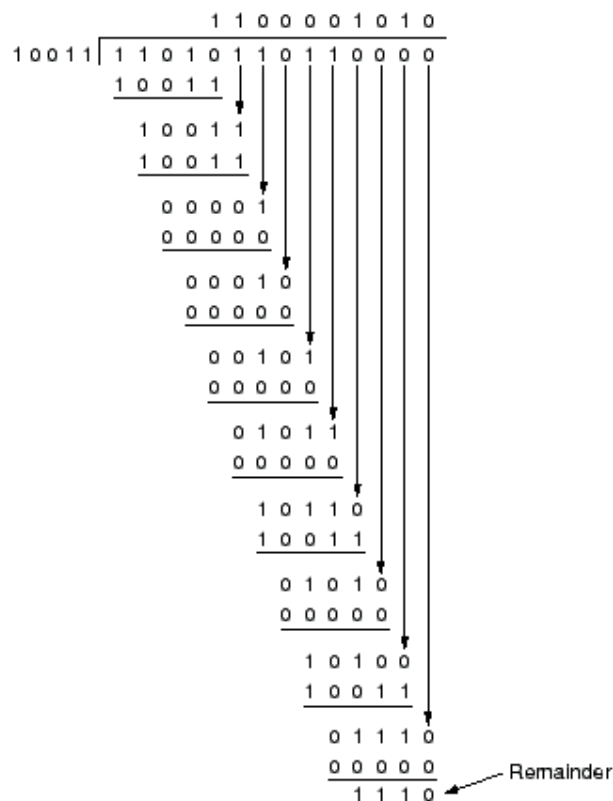
Frame : 1 1 0 1 0 1 1 0 1 1
Generator: 1 0 0 1 1
Message after appending 4 zero bits: 1 1 0 1 0 1 1 0 1 1 0 0 0 0

Transmitted frame: 1 1 0 1 0 1 1 0 1 1 1 1 1 0

Figura 2.1.6: Cálculo de polinômio de erro.

Apesar da aparente complexidade do cálculo manual do polinômio, ele é facilmente implementado em hardware. O polinômio gerador pode ser implementado utilizando-se portas ou-exclusivo, e flip-flops tipo D (células de memória), em uma configuração que permita um deslocamento dos bits. Esse código é utilizado basicamente em comunicações seriais. Uma aplicação em paralelo pode ser feita utilizando-se vários polinômios geradores, um para cada bit da informação paralela, transmitindo simultaneamente.

1.5 Correção de Erros

Para possibilitar uma comunicação sem erro não basta apenas detectar a ocorrência de erros. Assim é necessário desenvolver um mecanismo que corrija o erro detectado. A correção de erros pode ter dois enfoques: no primeiro o código de detecção carrega consigo informações suficientes para recuperar o erro (FEC) e no segundo quando o erro é detectado é solicitado a repetição da mensagem errada para regenerar a mensagem original (ARQ).

1.5.1 Código de Correção de Erros (FEC)

Em um sistema que utilize códigos de correção ou detecção de erros, um codificador gera uma palavra de código contendo a informação recebida e o código de correção (ou detecção) de erros para essa informação. As palavras de código fazem parte de um subconjunto em S de um universo em U de vetores. Uma falha pode fazer com que uma palavra de código produza uma outra palavra de código contendo erro. Se essa palavra de código fizer parte de em S, esse erro não será detectado, e se fizer parte de em U – S, então o erro será detectado.

Dependendo do código de correção de erros utilizado (bloco ou árvore), a palavra de código poderá ser algumas vezes maior que a informação original recebida pelo codificador. No momento de sua utilização, a palavra de código e decodificada, e no caso de conter erro, este será corrigido com o uso do código de correção recebido junto com a informação, e a informação fornecida volta a ser a mesma recebida pelo codificador.

Os códigos estão divididos em cíclicos e não-cíclicos. Os códigos cíclicos são aqueles em que uma rotação realizada na palavra de código gera uma nova palavra de código, o mesmo conceito não se aplica para códigos não-cíclicos.

O código de Hamming é descrito por uma matriz de verificação de paridade H, contendo m linhas e 2m – 1 colunas. Quando uma palavra de código X e transmitida, a palavra recebida será X + E, onde E representa o vetor erro. Se não ocorrer erros, o vetor erro sera igual a zero. Se ocorrer um erro, o vetor

E conterá apenas um bit 1, e os demais estarão em 0. O vetor recebido e verificado multiplicando pela matriz H. Assim, a verificação é função apenas do vetor erro E, e da matriz de paridade H. S e ocorreu um erro em um único bit, este estará representado por 1 no vetor E, e multiplicando-se esse vetor pela matriz H, obtém-se a linha da matriz e a palavra correta.

Um dos maiores problemas de se usar códigos de correção de erros, e que quanto maior a habilidade de corrigir erros, maior será o tamanho do código. Outro problema é quanto a complexidade matemática para implementação dos codificadores e decodificadores. Em comunicação via satélite, a latência de transmissão é muito grande, e a correção por protocolo é ineficiente, por isso costuma-se utilizar código de correção de erros.

Códigos Cíclicos

Os códigos cíclicos são os mais importantes, destacando-se, os códigos de Hamming, códigos BCH, códigos cíclicos de correção de erros em rajadas, entre outros. Todos esses códigos são determinados por estruturas algébricas como por exemplo polinômios, e seus codificadores e decodificadores devem ser projetados de acordo com suas especificações.

O projeto desses codificadores e decodificadores é feito com o uso dos conceitos básicos da teoria de circuitos elétricos, implementando as funções requisitadas pelos diversos tipos de códigos.

Códigos Não-Cíclicos

Alguns exemplos de códigos não-cíclicos são os códigos em concatenados, e os códigos de em baixa densidade. Códigos de Hamming, Golay e Reed--Muller são exemplos de códigos não-cíclicos, que possuem um correspondente cíclico.

1.5.2 Correção de Erro por Protocolo (ARQ)

Outra forma de corrigir erro é retransmitir a mensagem errada através do protocolo. Esse mecanismo é geralmente chamado ARQ ou repetição de requisição automática.

Stop-and-Wait ARQ (Para-e-Espera)

Assim como no controle de fluxo, o stop-and-wait ARQ envia um pacote e espera pela confirmação do receptor. Se houver erro ou o time-out expirar envia novamente a mensagem até receber uma resposta positiva ou esgotar o número de tentativas de retransmissão. Um exemplo do stop-and-wait ARQ quando há perda de uma mensagem é mostrado na Figura 2.1.7.

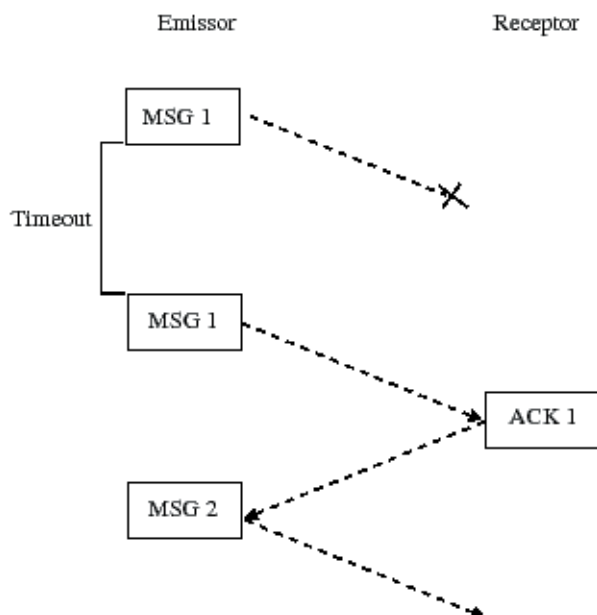



Figura 2.1.7: Exemplo do Stop-and-Wait ARQ quando uma mensagem é perdida.

Outro caso possível é a chegada correta da mensagem ao destinatário e a perda da mensagem de reconhecimento. Neste caso o remetente também não recebe o reconhecimento e retransmite a mensagem ao expirar o time-out. Agora, no entanto, o destinatário descarta a mensagem repetida e retransmite o reconhecimento. Um exemplo do stop-and-wait ARQ quando há perda de um reconhecimento é mostrado na Figura 2.1.8.

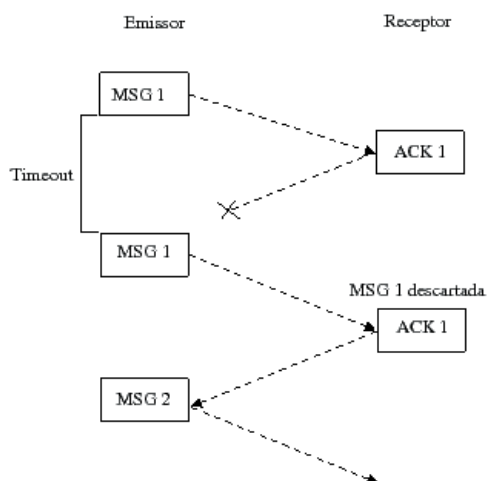



Figura 2.1.8: Exemplo do Stop-and-Wait ARQ quando um reconhecimento é perdido.

Go-back-N ARQ (Retransmite desde N)

Quando usamos um protocolo de janelas deslizantes podemos usar o go-back-N ARQ. O emissor envia uma janela de pacotes e aguarda a confirmação, quando envia novos pacotes mantendo a janela. Se houver erro ou o time-out expirar o transmissor envia novamente todas os pacotes a partir do pacote errado ou perdido (go-back-N). Este procedimento se repete até receber uma confirmação positiva ou esgotar o número de tentativas de retransmissão. O receptor recupera o pacote danificado e descarta os pacotes seguintes, caso tenha recebido perfeitamente.

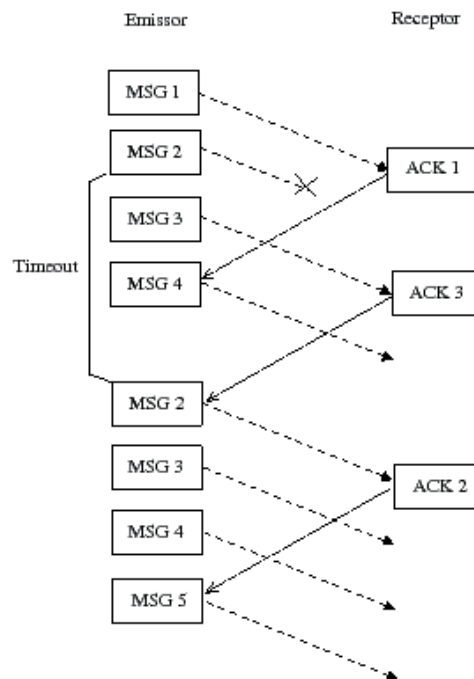



Figura 2.1.9: Go-back-N ARQ.

Um exemplo do go-back-N ARQ é mostrado na Figura 2.1.9. A janela de congestionamento é de três pacotes. O emissor envia três pacotes e transmite os demais com a chegada do reconhecimento. Nesse exemplo o pacote MSG 2 é perdido, então o emissor ao receber o reconhecimento ACK 3 ou expirar o time-out da MSG 2, envia novamente todos os pacotes a partir da MSG 2. O receptor então descarta todas as mensagens já recebidas e reconhecidas e aguarda pelas novos pacotes que chegarão.

Selective-Reject ARQ (Retransmissão Seletiva)

Outro procedimento de recuperação de erro para um protocolo de janelas deslizantes é o selective-reject ARQ. Quando houver erro ou o time-out expirar o emissor envia novamente apenas o pacote com erro. Este procedimento se

repete até receber uma confirmação positiva dessa mensagem ou se esgotar o número de tentativas de retransmissão. O receptor recupera o pacote perdido ou danificado e aguarda pelos pacotes seguintes.

Apesar da aparente eficiência desta técnica, na prática ela é muito parecida com o go-back-N pois a complexidade do mecanismo de selective--reject não compensa a economia de pacotes não transmitidos.

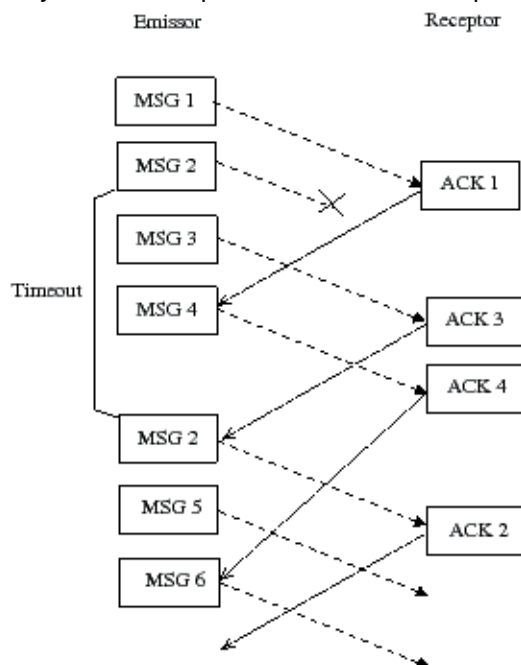



Figura 2.1.10: Selective-Reject ARQ.

Um exemplo do selective-reject ARQ é mostrado na Figura 2.1.10. A janela de congestionamento é de três pacotes. O emissor envia três pacotes e transmite os demais com a chegada do reconhecimento. Nesse exemplo o pacote MSG 2 é perdido, então o emissor ao receber o reconhecimento ACK 3 ou expira o timeout da MSG 2, envia novamente o pacote MSG 2. Note que os demais pacotes da janela continuam sendo transmitidos desde que seja mantido o tamanho da janela.

1.6 Desempenho de comunicação

Devido aos controles necessários para funcionamento de uma camada de enlace, não podemos aproveitar toda capacidade. Por exemplo, se o enlace tem uma capacidade de 1 MBPS nunca conseguiremos transmitir essa taxa útil. Os controles do protocolo e os tempos de espera reduzem a taxa possível.

$$t = \frac{Q}{c}$$

O tempo t é o tempo que se leva para transmitir um quadro de tamanho Q bits por uma linha com capacidade c bps.

$$r = \frac{c}{t}$$

Analogamente, a taxa efetiva r bps é calculada dividindo-se o tamanho do dado c bits pelo tempo de transmissão t segundos.

$$t = t_p + t_t$$

O tempo total t é igual ao tempo de propagação tp, que é o tempo que o sinal viaja pelo meio de transmissão, mais o tempo de transmissão Tt, isto é, o tempo em que o quadro completo é transmitido pelo meio.

$$Q = q_t - q_c$$

A quantidade de informação útil Q é igual a quantidade total qt menos a quantidade de informações de controle qc.

É importante lembrar que no cálculo de desempenho de um protocolo precisamos contabilizar o tempo da mensagem de confirmação. Quando consideramos protocolos de janela deslizante é necessário contabilizar o tamanho da janela na quantidade de dados e no tempo total.

Atividades de avaliação

1. Relacione os mecanismos de controle de fluxo e diga suas principais características.
2. Porque o controle de fluxo Para-e-Espera (Stop-and-Wait) não é eficiente para redes de alta velocidade e comunicação via satélite ?
3. Qual é a função de um código de detecção de erros? Explique seu mecanismo.
4. Relacione os mecanismos de controle de erro e diga suas principais características.
5. A correção de erros por retransmissão (ARQ) exige um tempo maior para a recuperação de erros. Qual é o valor mínimo deste tempo? (Considere os dois casos de erro de transmissão de um pacote com Stop-and-Wait ARQ).
6. Digas as vantagens e desvantagens da correção automática (FEC) e a correção de erros por retransmissão (ARQ). Por que a maioria dos protocolos de enlace atuais empregam essa última técnica?

2. Protocolos WAN

Podemos classificar os protocolos de enlace conforme sua aplicação, para redes de longa distância, para redes locais ou para redes sem fio. Apresentamos nesse capítulo os protocolos de enlace para redes de longa distância (WAN). A seção 6.1 apresenta o protocolo PPP, muito utilizado para conexões na Internet e a seção 6.2 o protocolo HDLC. A seção 6.3 mostra o protocolo Frame-Relay, e finalmente, a seção 6.4 mostra o protocolo ATM.

2.1 Protocolo PPP (Point-to-Point Protocol)

O PPP é um protocolo para transmissão de pacotes através de linhas seriais. O protocolo PPP suporta linhas síncronas e assíncronas. Normalmente ele tem sido utilizado para a transmissão de pacotes IP na Internet.

O PPP é projetado para transportar pacotes através de uma conexão entre dois pontos. A conexão entre os pontos deve prover operação full-duplex sendo assumido que os pacotes são entregues em ordem. Estas características são desejadas para que o PPP proporcione uma solução comum para a conexão de uma grande variedade de dispositivos, incluindo pontes (bridges) e roteadores (routers).

O PPP é composto basicamente de três partes, sendo que a interação entre elas obedece a um diagrama de estados.

2.1.1 Diagrama de estados do PPP

O diagrama de estados do protocolo PPP é mostrado na Figura 2.2.1. O estado REPOUSO corresponde ao estado neutro, aguardando uma conexão. Ao detectar a portadora inicia o estado CONEXTADO onde é usado o protocolo LCP. A próxima etapa, AUTENTICAÇÃO é responsável pela autenticação do usuário, utilizando algum protocolo específico (por ex., RADIUS). Se a autenticação for bem sucedida entra no estado CONFIGURAÇÃO DE REDE, onde negocia os parâmetros de rede (por ex., endereço IP) através do protocolo NCP. No estado COMUNICAÇÃO a conexão é estabelecida a nível de transporte. O estado ENCERRAMENTO encerra a conexão de Transporte e Rede e após a queda da portadora vai para o estado REPOUSO.

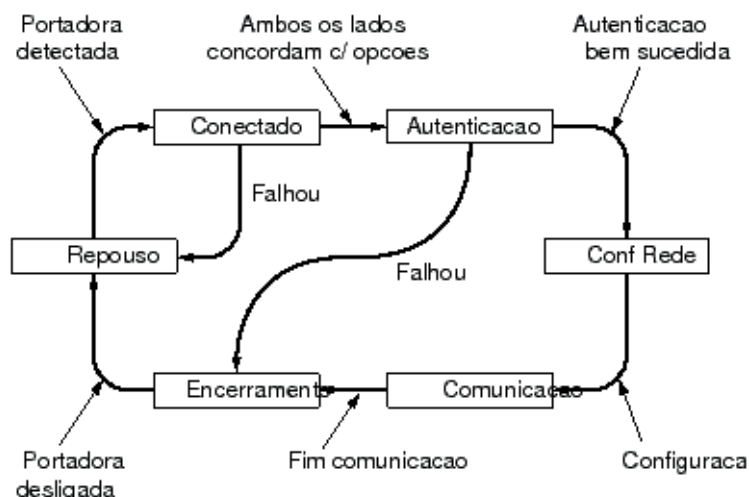



Figura 2.2.1: Diagrama de estados do protocolo PPP.

2.1.2 Encapsulamento

O encapsulamento do PPP provê multiplexação de diferentes protocolos da camada de rede simultaneamente através do mesmo link. Este encapsulamento foi cuidadosamente projetado para manter compatibilidade com os suportes de hardware mais comumente utilizados.

Somente 8 octetos adicionais são necessários para formar o encapsulamento do PPP se o compararmos ao encapsulamento padrão do quadro HDLC. Em ocasiões em que a largura de banda é crítica o encapsulamento e o quadro podem ser encurtados para 2 ou 4 octetos.

Para suportar implementações de alta velocidade, o encapsulamento padrão usa somente campos simples, desta forma o exame do campo para a demultiplexação se torna mais rápida.

Esquema de encapsulamento do PPP é mostrado na Figura 2.2.2.

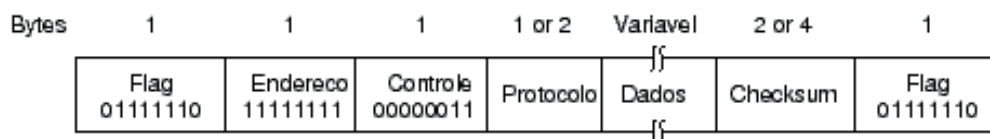



Figura 2.2.2: quadro do protocolo PPP.

2.1.3 Link Control Protocol - LCP

Para ser suficientemente versátil e portável para uma grande variedade de ambientes, o PPP provê um protocolo de controle - LCP.

O LCP é usado para automaticamente concordar sobre as opções de

formato de encapsulamento, lidar com variações nos limites de tamanho dos pacotes, detectar loops infinitos, detectar erros de configuração, iniciar e terminar a conexão.

Opcionalmente o LCP pode prover facilidades de autenticação de identificação e determinação de quando o link está funcionando apropriadamente ou quando está falhando.

2.1.4 Network Control Protocol - NCP

O NCP é composto por uma família de protocolos de rede. Ele estabelece e configura os diferentes protocolos na camada de rede que serão utilizados pelo PPP.

Links ponto-a-ponto tendem a agravar alguns problemas comuns a diversas famílias de protocolos de rede. Por exemplo, atribuição e gerenciamento de endereços IP é especialmente difícil sobre circuitos comutados com links ponto-a-ponto. Estes problemas são tratados pela família de NCP, onde é necessário um gerenciamento específico para cada problema.

2.2 HDLC (High-Level Data Link Control)

O protocolo HDLC é um protocolo de enlace orientado a bit para linhas seriais. É padronizado pela ISO, e foi desenvolvido a partir do protocolo SDLC da IBM, incorporando várias de suas funções.

A Figura 2.2.3 apresentam o formato do quadro do HDLC. Um dos objetivos do protocolo de enlace é transmitir transparentemente os dados da camada Rede. Como o HDLC é um protocolo orientado à bit, é necessário o preenchimento de bit se os dados contém alguma sequência igual ao flag, evitando que o protocolo interprete um flag de fim de quadro erroneamente.

Bits	8	8	8	≥ 0	16	8
	0 1 1 1 1 1 1 0	Address	Control	Data	Checksum	0 1 1 1 1 1 1 0

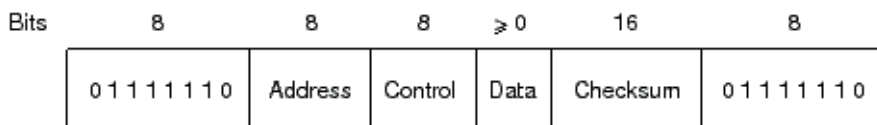



Figura 2.2.3: Formato do quadro HDLC.

O protocolo define três tipos de quadro, mostrado na Figura 2.2.4: quadros de informação (a), de supervisão(b) e não numerados (c). Os quadros são caracterizados pelo campo de controle, que possui diversas funções, dependendo do tipo de quadro.

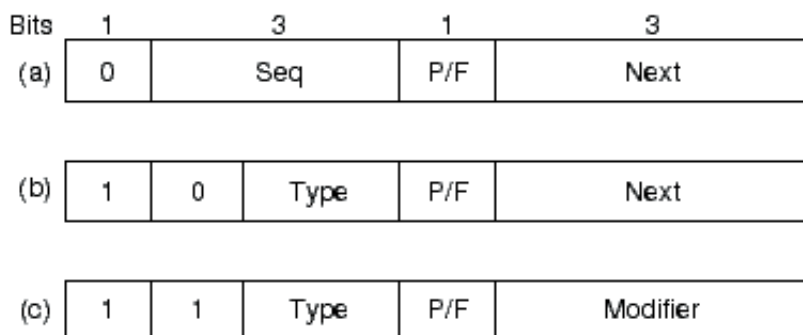



Figura 2.2.4: Tipo de mensagem de controle HDLC.

Os quadros de informação (a) possuem dois campos para numeração de sequência além do bit P/F. N(s) indica o número do quadro sendo transmitido. N(r) é a confirmação por carona, indicando o número do próximo quadro esperado na direção oposta. O tamanho máximo de janela no protocolo pode ser de 7 ou 127, correspondendo a três ou sete bits.

Os quadros de supervisão (b) fornecem o mecanismo de ARQ (Automatic Repeat reQuest, pedido automático de repetição) quando a carona não é utilizada. O quadro Receiver Ready (RR) é utilizado para confirmar o recebimento de um quadro e para indicar que o receptor está ativo, pronto para receber informação. É utilizado como comando e como resposta. Já o quadro Receiver Not Ready (RNR) confirma o quadro recebido, mas indica que o transmissor deve aguardar para transmitir um outro quadro. Quando estiver pronto ele envia um RR e a troca de dados se reinicia. Os quadros de comando Reject (REJ) e Selective Reject (SREJ) são utilizados para rejeitar explicitamente quadros nos mecanismos de retorna a N e retransmissão seletiva respectivamente.

Os quadros não numerados são utilizados para gerência da conexão. Não possuem numeração de sequência, não alterando portanto a janela. Temos quatro grupos distintos de comandos. Existem quadros para determinação do modo de funcionamento como SNRM (Set Normal Response Mode), DISC (Disconnect), SABM (Set Asynchronous Balance Mode), para transferência de informações entre estações como UP (Unnumbered Poll) utilizado para solicitar informações de controle, UA (Unnumbered Ack) utilizado para confirmar os quadros desta categoria, quadros para recuperação quando o mecanismo de ARQ não se aplica como FRMR (Frame Reject), por exemplo para rejeitar um quadro com campo de controle inválido, e quadros de aplicação variada como XID, para troca de estado e identificação entre estações e TEST para teste do circuito.

O bit P/F possui significados diferentes dependendo se o quadro é de comando ou de resposta, e dependendo do modo de operação. Quando ope-

rando em modo de resposta normal, a secundária só pode transmitir após receber um comando com P=1, indicando um Poll. A primária solicita dados enviando um quadro com P=1, ou quadros de supervisão, como RR, REJ ou SREJ com P=1. Se o quadro é de resposta e F=1 (é o mesmo bit, mas agora com outro significado), isso indica que este é o último quadro de informação a ser transmitido, e a linha pode ser liberada para outra estação.

Existem vários protocolos de enlace orientados a bit semelhantes ao HDLC. Podemos citar o LAPB, utilizado na “família” X.25, que utiliza apenas o modo assíncrono balanceado do HDLC, o LLC, padronizado pela IEEE para uso em redes locais, e que também utiliza o modo assíncrono balanceado do HDLC. Existe também o SDLC, que inclusive deu origem ao HDLC, e que utiliza o modo de resposta normal e possui alguns comandos não definidos no HDLC.

2.3 Frame-Relay

Quando se pensa em uma rede comutada a pacotes o X.25 foi um dos primeiros exemplos e foi largamente utilizado. Não apenas pela razão histórica mas porque ele serviu de referência para várias outras tecnologias como Frame Relay e ATM.

O protocolo X.25 segue as seguintes diretivas:

1. O canal de controle compartilha o mesmo canal de dados, o que chamamos sinalização inband.
2. A multiplexação dos canais virtuais se encontram na camada 3.
3. As camadas 2 e 3 implementam controle de fluxo e de erro.

Entretanto, essa arquitetura provoca uma considerável sobrecarga no protocolo, limitando a velocidade máxima para essa tecnologia em 64 Kbps. O Frame Relay, no entanto, seguiu as seguintes diretivas:

1. O canal de controle utiliza um canal separado ao de dados.
2. A multiplexação dos canais virtuais se encontram na camada 2, eliminando uma camada inteira de processamento.
3. Não existe controle de fluxo e de erro nessas camadas, ficando sob a responsabilidade das camadas superiores.

Com essa nova arquitetura conseguimos atingir velocidades de até 2 Mbps.

2.3.1 Arquitetura

O Frame-Relay oferece um serviço de qualidade razoável por um bom custo,

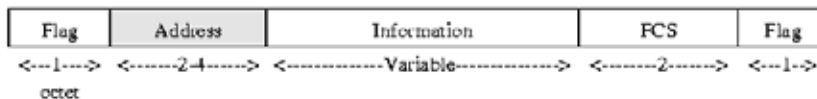
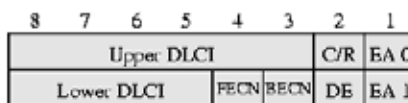
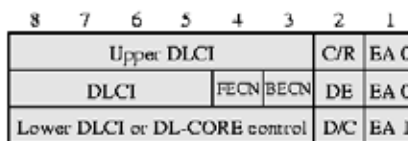
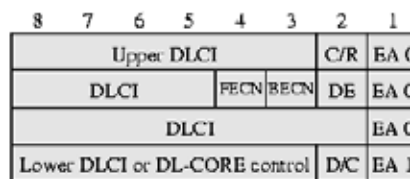
por isso cada vez mais tem crescido seu uso, apesar de não ser o mais moderno (posto ocupado pelo ATM). O serviço Frame Relay é composto de dois itens: acesso e CIR.

Todo usuário precisa ser ligado a rede, por isso ele contrata uma porta ao provedor de serviço. No entanto esse acesso não garante a entrega do entrega do pacote ao destino, por isso é necessário contratar um CIR, que é uma taxa garantida ponto a ponto. Assim temos um serviço ótimo para o valor do CIR e um serviço razoável para o resto da banda do acesso, que será transmitido apenas caso a rede suporte, por um preço bem inferior a uma linha dedicada e até mesmo ao X.25. Como a natureza do tráfego de dados geralmente tem um padrão de rajadas essa característica não atrapalha.

Não existe endereço de rede, apenas o canal por onde o pacote deve seguir. Esse canal é chamado DLCI, que pode ter o número diferente em cada ponta da conexão. O controle é feito pelo canal de sinalização, que foi padronizado como DLCI = 0.

2.3.2 Cabeçalho Frame Relay

8 7 6 5 4 3 2 1

Upper DLCI			C/R	EA 0
DLCI	FECN	BECN	DE	EA 0
Lower DLCI or DL-CORE control			D/C	EA 1

(c) Address field - 3 octets

EA Address field extension bit
C/R Command/response bit
FECN Forward explicit congestion notification
BECN Backward explicit congestion notification
DLCI Data link connection identifier
D/C DLCI or DL-CORE control indicator
DE Discard eligibility

Figura 2.2.5: Cabeçalho Frame Relay.

O cabeçalho Frame Relay é mostrado na Figura 2.2.5. Existem vários tipos de cabeçalho, com 2, 3 ou 4 bytes de comprimento, e o que diferenciam basicamente é a quantidade de DLCIs possíveis de serem usados nos dispositivos de conexão da rede. O tamanho do DLCI pode ser 10, 17 ou 24 bits (respectivamente 1.024, 131.072 e 16.777.216 DLCIs). O tamanho do DLCI é definido pelos bit EA, que se for 1 indica o término do cabeçalho.

O bit C/R é utilizado pela aplicação, portanto sem uso para o protocolo. O bit D/C indica se os útimos seis bits do cabeçalho são DLCI ou controle do núcleo (core) do protocolo LAPF. Os bits FECN, BECN e DE são utilizados para controle de congestionamento.

2.3.3 Controle de Congestionamento

Os objetivos do controle de congestionamento do Frame Relay foram:

- Minimizar perda de pacotes.
- Manter a qualidade de serviço contratada com um mínimo de variação.
- Dividir os recursos de rede justamente, isto é, não permitir que um usuário monopolize a rede para si.
- Ter implementação simples para permitir velocidades altas.
- Minimizar a variação de qualidade de serviço quando um congestionamento for eminente.

O bit DE indica que o pacote é candidato ao descarte, isto é, se ocorrer um congestionamento em algum ponto da rede, primeiro serão eliminados os pacotes marcados com bit DE. Esse bit é marcado pelos equipamentos de borda (onde os usuários estão ligados) quando o tráfego entrante ultrapassar o valor do CIR. Vale lembrar que esse valor é calculado por um período, isto é, se o canal foi pouco usado por um tempo, ele aceita uma rajada de pacotes sem marcar o bit DE.

Os bits BECN e FECN são usados para evitar congestionamento. O BECN indica que há uma possibilidade de haver congestionamento no sentido contrário ao de recebimento do pacote. Assim, se um receptor recebe um pacote com bit BECN marcado ele deve diminuir a taxa de resposta para evitar o congestionamento.

O FECN indica que há uma possibilidade de haver congestionamento no sentido de recebimento do pacote. O receptor devolve uma mensagem para o transmissor com bit FECN marcado. Assim se o transmissor recebe um pacote com bit FECN marcado ele deve diminuir a taxa de transmissão para evitar o congestionamento.

2.4 ATM

O ATM ou Modo de Transmissão Assíncrono, é uma tecnologia baseada na transmissão de pequenos pacotes de tamanho fixo e estrutura definida denominados células. Estas células são transmitidas através de conexões de circuitos virtuais estabelecidos, sendo sua entrega e comutação feitas pela rede baseado na informação de seu cabeçalho. Esta tecnologia se adapta facilmente às exigências de uma grande gama de tráfegos, suportando com isto diferente tipos de serviços. Com isto, a tecnologia ATM foi escolhida de forma a dar suporte à implantação da Rede Digital de Serviços Integrados - Faixa Larga RDSI-FL (Broadband Integrated Services Network - B ISDN).

Não há como se falar de redes ATM sem se ater por alguns momen-

tos em redes RDSI-FL. Na verdade a história e evolução das redes ATM, bem como a sua normalização através das recomendações do CCITT (atual ITU-T), aconteceram dentro do contexto da evolução da Rede Digital de Serviços Integrados - Faixa Larga. Os próximos tópicos deste hipertexto abordam o desenvolvimento da RDSI-FL, e por conseguinte, o desenvolvimento das redes ATM.

2.4.1 Modelo de Referência

A definição do modelo de referência segue a estrutura hierarquizada do modelo de referência OSI. A arquitetura de referência para a utilização de ATM é apresentada na Figura 2.2.6.

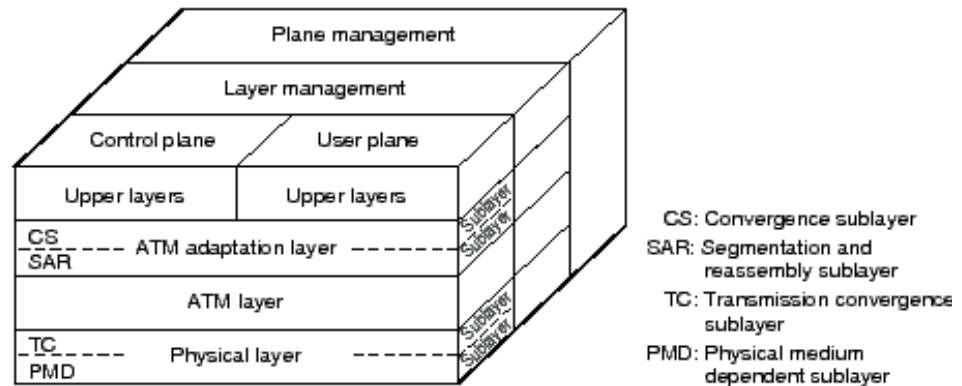



Figura 2.2.6: Modelo de Referência do ATM.

O modelo utiliza o conceito de planos distintos a fim de separar funções de usuário, de gerenciamento e de controle. O plano de gerenciamento seria responsável pela manutenção da rede e execução de funções operacionais, gerenciando os demais planos e a si próprio; o plano do usuário seria responsável pelo transporte de informações do usuário; por fim, o plano de controle seria responsável pelas informações de sinalização da rede.

O plano do usuário é dividido em três camadas inferiores e camadas superiores. As camadas superiores não são objetos de definição das recomendações para a RDSI-FL. As camadas inferiores são a Camada Física, Camada ATM, e a Camada de Adaptação.

A camada física corresponde funcionalmente à camada física do modelo de referência OSI, apresentando as características relacionadas ao meio físico de transmissão. A camada ATM é responsável pelo transporte de células ATM, possuindo independência em relação às idiossincrasias do meio físico utilizado. A camada de adaptação ATM tem como função mapear as informações do protocolo de nível superior em células ATM. Tipos diferentes de protocolos para a camada de adaptação ATM são definidos, levando-se em consideração as diferentes características dos serviços que são oferecidos.

2.4.2 Camada ATM

A camada ATM, assim como a camada física, toma parte no funcionamento de todos os elementos da rede, incluindo os comutadores. As funções desta camada, especificadas pela recomendação I.150, incluem:

Controle de fluxo Multiplexação/demultiplexação de células Tratamento dos cabeçalhos das células Roteamento das células baseados nas informações do cabeçalho A camada ATM faz todo o seu processamento a partir da geração e inspeção dos campos de cabeçalho da célula ATM. As informações sobre o formato das células, bem como o comutação das mesmas estão contidas na recomendação I.361.

2.4.3 Campos da célula ATM

Os campos VCI e VPI são os campos necessários para que os comutadores possam efetuar a comutação das células. O campo PT identifica o tipo de célula, onde os significados são apresentados na tabela 2.2.1.

Tabela 2.2.1

Significado do campo PT do cabeçalho ATM	
Código PT	**Significado**
0 0 0	Célula de informação de usuário que não passou por congestionamento no caminho.ATM-user-to-user indication =0.
0 0 1	Célula de informação de usuário que não passou por congestionamento no caminho.ATM-user-to-user indication =1.
0 1 0	Célula de informação de usuário que passou por nó em congestionamento. ATM-user-to-user indication =0.
0 1 1	Célula de informação de usuário que passou por nó em congestionamento. ATM-user-to-user indication =1.
1 1 0	Célula associada ao fluxo de segmento.
1 0 1	Célula associada ao fluxo fim-a-fim.
1 1 0	Célula de gerenciamento de recursos.
1 1 1	Reservado para uso futuro.

Qualquer nó congestionado pode modificar, assim que recebe a célula, o seu cabeçalho de forma a indicar que a célula passou por um nó em congestionamento.

O campo CLP indica a prioridade para o descarte de células pelos comutadores. O valor CLP=1 para uma célula implica em que, caso o nó tenha que descartar, esta célula será descartada primeiro.

O campo HEC é utilizado para a verificação de erros de transmissão. O HEC permite à camada física a verificação da integridade do cabeçalho.

O campo GFC aparece somente no cabeçalho das células UNI. Algumas alternativas para uso deste campo seriam para marcar como ociosa a célula, ou para marcá-la como sendo de informação de manutenção e operação da camada física.

Atividades de avaliação

1. Com relação ao estabelecimento de uma conexão PPP, diga qual a função dos protocolos LCP e NCP.
2. Quais as principais diferenças filosóficas do protocolo X.25 e Frame Relay?
3. Qual a utilidade do CIR em uma ligação Frame Relay?
4. Relacione os objetivos do controle de congestionamento do Frame Relay.
5. Descreva os controles de congestionamento reativo e preventivo do Frame Relay.
6. Uma célula ATM maior privilegiaria que tipo de tráfego? Por que? Que consequências isto traria para os outros tipos de tráfego?
7. Uma célula ATM menor privilegiaria que tipo de tráfego? Por que? Quais consequências isto traria para os outros tipos de tráfego?
8. O cabeçalho da célula ATM tem o campo HEC de um byte usado para proteção contra erros no cabeçalho. O campo dados do usuário não tem proteção. Explique por que?

3. Protocolos LAN

A multiplexação do acesso ao meio físico no nível de enlace é realizada através da identificação dos usuários do enlace, isto é, da identificação dos pontos de acesso a serviços SAP. Desta forma, o protocolo LLC deve identificar qual o ponto de acesso origem SSAP e qual o ponto de acesso destino DSAP. O padrão IEEE 802 estabelece como cada entidade das redes locais se comunica com seu nível superior (serviços prestados) e qual o protocolo utilizado para se comunicar com as entidades pares. O padrão IEEE 802.2 refere-se ao o protocolo para a camada LLC.

3.1 Aloha

Um dos primeiros protocolo LAN foi conhecido como Aloha, pois foi desenvolvido na Universidade do Hawai em 1970. Esta universidade apresentava uma característica única, várias unidades em diversas ilhas com dificuldade de comunicação via cabo, por isso usava rádio comunicação.

O protocolo é muito simples, se alguém quiser mandar uma mensagem para outro devia enviá-la. Se o receptor estivesse pronto recebia a mensagem sem problema. Quando houver colisão retransmite novamente. O diagrama de mensagens é mostrado na Figura 2.3.1.

User
A
B
C
D
E
Time

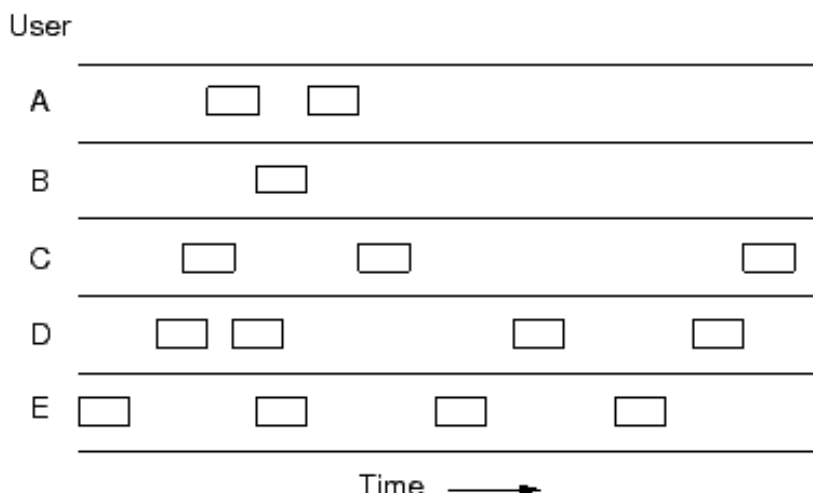



Figura 2.3.1: Transmissão Aloha puro.

Podemos observar que enquanto a rede fosse pouco utilizada o funcionamento é muito bom, mas se o tráfego aumentar a taxa de colisão crescerá exponencialmente e a comunicação se tornará muito difícil. Isso porque o tempo de transmissão de uma mensagem é maior que o tempo de espera.

Mais tarde esse protocolo sofreu uma modificação para melhorar a eficiência e foi conhecido como Slotted Aloha. Agora o tempo de transmissão é fixo (um slot) e qualquer estação só podia transmitir uma mensagem neste slot e a mensagem não podia ultrapassar esse tempo (é claro que podia ser fragmentada em vários pedaços). Com isso a probabilidade de colisão diminuiu e o rendimento aumentou.

Apesar do esquema simples e aparentemente ineficiente, o protocolo Aloha ainda é muito usado em comunicação via satélite, porque a latência (tempo de viagem de um pacote) é muito grande e qualquer controle de contenção (por exemplo, como no Ethernet) não melhora o resultado final.

3.2 Ethernet

3.2.1 Introdução

O protocolo Ethernet surgiu nos laboratórios da Xerox em 1976. Aproveitando a ideia do Aloha foi incluído algumas melhorias:

1. Uma estação ouve o meio (cabo) antes de transmitir.
2. Quando o cabo silencia, transmite a mensagem.
3. Se por acaso outra estação também estava querendo transmitir no mesmo instante há uma colisão. Por isso após iniciar a transmissão continua escutando a linha para verificar se não há colisão.

4. Se houver colisão, para de transmitir e espera um tempo aleatório antes de tentar nova transmissão.

O sucesso foi tão grande que outros fabricantes adotaram também e posteriormente o IEEE publicou a norma 802.3 que padronizou o Ethernet possibilitando a interoperabilidade. Esta norma implementa o controle CSMA/CD (Carrier Sense Multiple Access - Colision Detect).

3.2.2 Estados do CSMA/CD

A Figura 2.3.2 mostra os três estados possíveis do CSMA/CD:

Transmitindo

- Quando uma estação está transmitindo uma mensagem.

Espera

- Nenhuma estação está transmitindo.

Contenção

- Período que uma estação deve esperar para verificar se não tem ninguém transmitindo (tempo de propagação da estação mais distante, geralmente o comprimento máximo do cabo).

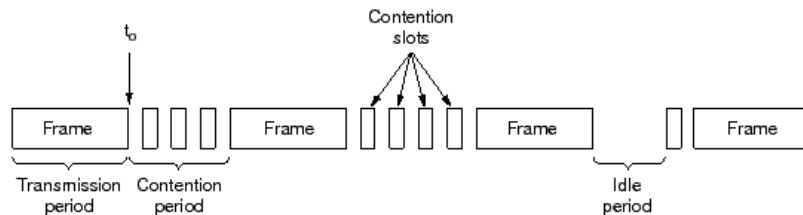



Figura 2.3.2: Estados do CSMA/CD.

3.2.3 Tipos de cabeamento

A norma Ethernet permite quatro tipos de cabeamento:

Coaxial Grosso:

Primeiro tipo de cabeamento usado, mostrado na Figura 2.3.3a, consiste em um cabo coaxial grosso (Thick Ethernet ou 10Base5) geralmente na cor amarela (por isso também é conhecido como Yellow Cable). A ligação com a estação é feita através de um conector vampiro e um transceiver AUI. Permite 100 nós a uma distância máxima de 500 m.

Coaxial Fino:

Como o cabo coaxial grosso é muito caro, foi criada uma alternativa barata usando um cabo mais fino, mostrado na Figura 2.2.3b, também conhecido como Thin Ethernet ou 10Base2. A ligação com a estação é feita através

de um conector BNC sem tranceiver (mais barato). Permite 30 nós a uma distância máxima de 180 m.

Par trançado:

O cabo coaxial fino apresenta problema de manutenção, pois basta um conector mal colocado e toda a rede para de funcionar. Assim foi utilizado cabo par trançado, parecido com os cabos telefônicos, mostrado na Figura 2.3.3c, também conhecido como 10BaseT. Agora é necessário utilizar um repetidor ativo chamado Hub, porém o custo final é semelhante ao coaxial fino com a vantagem de melhor confiabilidade. Permite 1024 nós a uma distância máxima de 100 m.

Fibra Ótica:

É a solução mais cara mas que possibilita distâncias maiores e pode ser usado para interligar prédios. Esse padrão é conhecido como 10BaseFL. Também é necessário utilizar um Hub, pois a ligação é ponto-a-ponto. Permite 1024 nós a uma distância máxima de 2000 m.

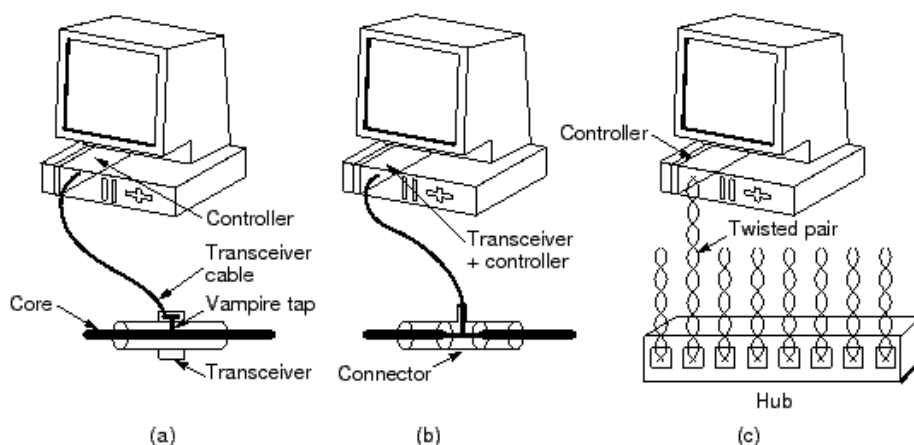



Figura 2.3.3: Tipos de cabeamento Ethernet.

3.2.4 Codificação

O 802.3 usa codificação Manchester com níveis de +0,85 V e -0,85 V, propiciando um nível DC de 0 V.

3.2.5 Subcamada MAC

A Figura 2.3.4 mostra um quadro 802.3 que tem os seguintes campos:

Preâmbulo:

Todo quadro começa com um preâmbulo que consiste em 7 bytes com o padrão de bit 10101010, para permitir que o receptor sincronize o relógio.

Delimitador de quadro:

Para indicar o início do quadro útil. Consiste em um byte 10101011.

Endereço de Destino:

Indica o endereço da estação de destino. O endereço é composto de 6 bytes.

Endereço de Origem:

Indica o endereço da estação de origem. O endereço é composto de 6 bytes.

Tamanho do campo de dados:

O Ethernet permite tamanho de dados variável, e este campo pode ter valores de 0 a 1500 bytes. Por questões práticas o quadro não pode ter menos de 64 bytes, pois as demais estações confundem o quadro com uma colisão.

Dados:

O conteúdo útil do quadro com tamanho máximo 1500 bytes.

Pad:

Se a mensagem útil for menor que 46 bytes este campo completa o tamanho do pacote para atingir o mínimo de 64 bytes.

Checksum:

Código de verificação de erro, no qual é utilizado o CRC-32.

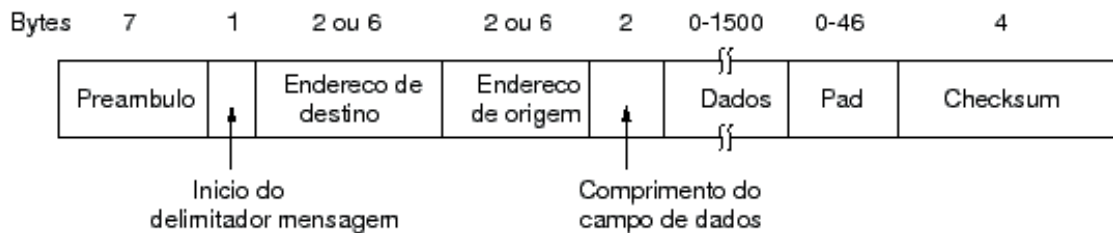



Figura 2.3.4: Formato do quadro Ethernet (802.3).

3.2.6 Algoritmo Backoff Binário Exponencial

Se duas estações quiserem enviar mensagem, eles vão tentar mandar logo após o término da transmissão da mensagem corrente, que vai provocar uma colisão. Detectando a colisão ambos param de transmitir e vão tentar novamente, mas agora segue a seguinte regra:

1. É determinado o tempo de slot que é função da distância do segmento da rede. No entanto, é comum usar o valor determinado na 802.3 que é 51,2 microsegundos. Esse é o tempo de um cabo ótico com 2,5 Km de comprimento e 4 repetidores.

2. Após a primeira colisão cada estação escolhe randomicamente o valor 0 ou 1. Se for 0 transmite imediatamente, senão espera um período 51,2 microsegundos. A probabilidade de colisão é 50%.
3. Se os dois escolherem o mesmo número, ocorrerá nova colisão. Agora cada estação vai tentar transmitir novamente, mas escolhendo um número randômico entre 0 e 3 (22). Agora a probabilidade da colisão ocorrer é 25%.
4. Se os dois escolherem o mesmo número, ocorrerá nova colisão. Agora cada estação escolhe um número randômico entre 0 e 7 (23). A probabilidade da colisão ocorrer agora é 12,5%.
5. Se ocorrer colisão, aumenta o número randômico até um máximo de 1023, onde a probabilidade de que duas estações escolham o mesmo número é mínimo.

Esse algorítimo, permite o controle de colisão tentando aproveitar da melhor maneira o espaço de tempo, transmitindo mais rapidamente possível.

3.3 Fast-Ethernet (100BaseT)

O padrão 100 Base-T de Ethernet a 100Mbit/s mantém as principais características do padrão Ethernet 10Mbit/s, tais como o formato do quadro, a quantidade de dados que um quadro pode carregar, e o mecanismo de controle de acesso ao meio, diferenciando do padrão original apenas na velocidade de transmissão dos pacotes, que no padrão 100 Base-T é 10 vezes maior que no original.

Nas seções abaixo serão apresentadas as principais características deste padrão Fast Ethernet.

3.3.1 Meios Físicos para transmissão a 100Mbit/s

Há três meios que foram especificados para transmitir sinais Ethernet a 100Mbit/s: 100BaseT4, 100BaseTX e 100BaseFX. É sempre bom lembrar que “100” indica que a velocidade do meio é de 100Mbit/s, e “Base”, significa que o tipo de sinalização é a banda básica, ou seja, apenas sinais Ethernet são transmitidos no meio. Já T4, TX e FX identificam o meio físico utilizado.

O tipo T4 utiliza quatro canais de par trançado tipo telephone grade (UTP - Categoria 3), suportando somente transmissões half-duplex. O tipo TX utiliza dois cabos de par trançado tipo data grade (UTP ou STP Categoria 5), suportando transmissões a half-duplex ou full-duplex. O tipo FX utiliza fibra ótica, com transmissão a half-duplex ou full-duplex. Os padrões TX e FX são coletivamente conhecidos como 100Base-X. Os meios padrões 100Base-TX e 100Base-FX, usados no Fast Ethernet, foram originalmente desenvolvidos

pela ANSI (American National Standards Institute), para o padrão FDDI (Fiber Distributed Data Interface), e são amplamente utilizadas em redes locais FDDI. O padrão T4 foi provido para tornar possível o uso de fios de par trançado de baixa qualidade para sinais Ethernet a 100 Mbit/s.

Meio Físico

O meio físico usado para carregar sinais Ethernet entre os computadores pode ser um dos três tipos de meios a 100 Mbit/s apresentados na sub-seção anterior. A conexão ao meio físico é feita através da interface dependente do meio (MDI). A MDI consiste em um conector de par trançado ou de fibra ótica de oito pinos.

Dispositivo da Camada Física

Este dispositivo realiza as mesmas funções gerais de um transceptor do sistema Ethernet 10Mbit/s. Ele pode ser um conjunto de circuitos integrados dentro de uma porta Ethernet de um dispositivo de rede, portanto invisível ao usuário, mas também pode ser uma pequena caixa equipada com um cabo MII (Interface Independente do Meio), como o transceptor outboard e o cabo transceptor usados no Ethernet 10 Mbit/s.

Interface Independente do Meio

A Interface Independente do Meio (MII) é um conjunto de eletrônicos opcionais que provêm uma maneira de ligar as funções de controle de acesso ao meio do dispositivo de rede com o Dispositvo da Camada Física (PHY), o qual envia os sinais para o meio físico. A MII pode, opcionalmente, suportar tanto operações a 10Mbit/s como a 100 Mbit/s, permitindo que dispositivos de rede convenientemente equipados possam conectar tanto segmentos 10Base-T como 100Base-T.

O MII é projetado para tornar transparente ao chips Ethernet do dispositivo de rede, as diferenças de sinalização entre os vários tipos de meio físico . O MII converte o sinal recebido dos vários segmentos de meios pelo transceptor (PHY) em sinais no formato digital que então são providos ao chips Ethernet dos dispositivos. O MII opcional , o conector fêmea de 41 pinos a ele associado e o cabo MII, tornam possível conectar um dispositivo de rede a qualquer um dos diferentes tipos de meio, provendo assim uma maior flexibilidade.

Equipamento de Terminal de Dados

O dispositivo de rede é definido como um equipamento de terminal de dados (DTE) pelo padrão IEEE. Cada DTE ligado a um canal Ethernet é equipado com uma interface Ethernet. A interface Ethernet provê uma conexão ao meio

Ethernet e contém os eletrônicos e software necessários para realizar as funções de controle de acesso ao meio necessárias para enviar um quadro ao canal Ethernet.

É importante notar que as portas Ethernet dos repetidores não usam uma interface Ethernet. Uma porta do repetidor conecta-se ao sistema do meio FastEthernet usando os mesmos equipamentos PHY e MDI. No entanto, as portas dos repetidores operam ao nível de bit individual para sinais Ethernet, movendo os sinais diretamente de segmento para segmento. Entretanto, as portas dos repetidores não contêm interfaces Ethernet já que elas não operam ao nível de quadros Ethernet.

Por outro lado, um hub deve ser equipado com uma interface Ethernet para prover uma maneira de se comunicar com o hub através da rede. Isto permite que os vendedores ofereçam uma interface de gerenciamento no hub que possa interagir com uma estação de gerenciamento remota, usando o protocolo SNMP. Hubs gerenciados tornam possível que um gerenciador de rede monitore, remotamente, os níveis de tráfego e condições de erro nas portas do hub, ou desligue portas para depurar problemas.

3.4 FDDI (Fiber Distributed Data Interface)

Em 1980, com a finalidade de desenvolver uma rede de alto desempenho de propósito geral, foi formado um grupo de trabalho chamado de ANSI X3T9.5. Em junho de 1983, foram submetidas as primeiras propostas para os níveis físico (PHY) e de acesso (MAC), para que fosse desenvolvida uma interface de dados de alta velocidade baseada no uso de fibra ótica.

FDDI é um padrão designado pelo National Standards Institute (ANSI) comitê X3T9.5, com a participação de várias empresas de produtos e serviços de computação e telecomunicações. É uma rede em duplo anel usando fibra ótica como meio físico para transmissão de dados a uma taxa de 100 Mbps.

3.4.1 Arquitetura FDDI

FDDI emprega um esquema de acesso token-passing em um meio de fibra ótica para obter taxas de 100 Mbps. Conforme o padrão PMD (Physical Layer Medium Dependent), a transmissão se faz com diodos emissores de luz (LED), transmitindo em um comprimento de onda nominal de 1.300 nanômetros.

A conexão aos dois anéis de fibra é realizada através de conectores duplex polarizados. Cada estação pode se ligar diretamente ao meio, através da conexão aos dois anéis (estações de classe A), sendo exigido nesse caso dois cabos duplex, um para cada estação adjacente. Conexões mais simples podem ser realizadas (estações de classe B), requerendo apenas um cabo duplex, mas, por questão de confiabilidade, aconselha-se a conexão de tais

estações , através de um concentrador se ligando aos dois anéis. Também os concentradores têm características análogas às estações de classe A e B para ligação ao duplo anel. Na Figura 2.3.5 apresentamos um anel duplo FDDI em funcionamento normal (a) e quando ocorre uma falha no cabo interrompendo-o (b).

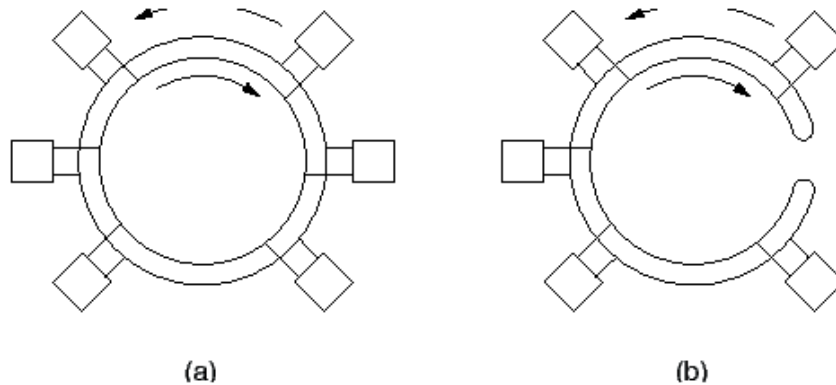



Figura 2.3.5: Arquitetura Física da FDDI.

3.4.2 Protocolo FDDI

Os protocolos FDDI correspondem aos níveis físico e de enlace do modelo OSI. O controle de acesso ao meio (MAC) foi especificado de forma a ser compatível com o protocolo LLC, padrão IEEE 802.2. MAC e LLC formam o nível de enlace conforme o modelo OSI. Os vários protocolos são:

PMD - Physical Layer Medium Dependent:

Especifica o enlace de fibra ótica e os componentes óticos relacionados, incluindo os níveis de potência e características dos transmissores e receptores óticos, os requisitos de sinais da interface ótica e a taxa de erros permissíveis.

PHY - Physical Layer Protocol:

Especifica os algoritmos de codificação/decodificação e de sincronismo de relógios e de quadros de dados.

MAC - Medium Access Control:

Especifica as regras de acesso ao meio, de endereçamento e de verificação de dados.

LLC - Logical Link Control:

Especifica as regras para troca de informação em serviços com conexão, sem conexão/sem reconhecimento e sem conexão/com reconhecimento.

SMT - Station Management:

Especifica o controle requerido para a operação apropriada das estações no anel, incluindo gerenciamento de configuração (manutenção, isolamento e recuperação de falhas, administração de endereços etc.), gerenciamento de conexão (alocação de banda passante etc.) e gerenciamento do anel (iniciação, monitoração de desempenho, controle de erro etc.).

3.4.3 FDDI - Controle de Acesso ao Meio

O protocolo FDDI distingue três tipos de tráfego: síncrono, assíncrono restrito e assíncrono não restrito.

Tráfego Síncrono:

Embora não garanta um retardo de transferência constante, o protocolo garante uma banda passante para os dados transmitidos e, também, um retardo de transferência limitado.

Tráfego Assícrono Restrito:

O protocolo não garante nenhum limite superior para o retardo de transferência. A banda passante não utilizada pelo tráfego síncrono é alocada para o tráfego assíncrono, onde é usada por um número limitado de estações.

Tráfego Assíncrono Não Restrito:

O protocolo também não garante nenhum limite superior para o retardo de transferência. A banda passante que não é utilizada pelo tráfego síncrono é alocada para o tráfego assíncrono, onde pode ser usada por todas as estações.

3.4.4 FDDI - Formato dos Quadros

Na arquitetura de protocolos FDDI, os dados são codificados para transmissão pelo protocolo PHY, usando a codificação 4 entre 5 (4B/5B/NRZI).

FDDI - Codificação

A codificação usada para transmissão de símbolos é a NRZI, onde 1 é representado por uma transição e 0 é por não haver transição. Como a codificação 4 entre 5 garante que nunca vai haver mais do que três zeros seguidos, nunca vai haver mais do que três tempos de bits sem haver transição, propriedade que é usada para o sincronismo entre os receptores e transmissores.

FDDI - Quadros MAC

Informações são transmitidas no anel FDDI em quadros MAC. A Figura 2.3.6 mostra o formato do quadro de dados.

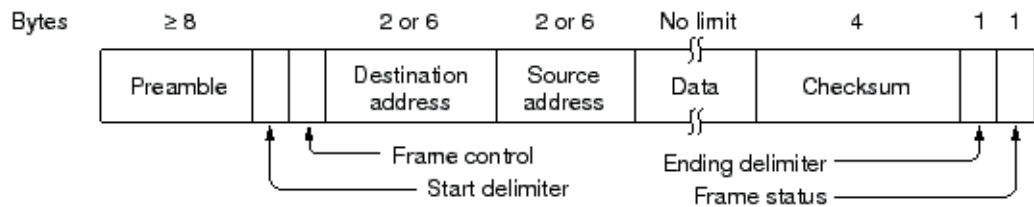



Figura 2.3.6: Quadro FDDI.

O preâmbulo (PA) precede cada transmissão e é usado para sincronismo entre o transmissor e o receptor. O delimitador de início de quadro (SD) consiste nos símbolos reservados JK. O campo FC (controle de quadro) define o tipo de quadro e sua característica. Ele distingue quadros síncronos e assíncronos, o comprimento do campo de endereço, e o tipo de quadro: se de informação (vindo da camada superior LLC), de controle de acesso (MAC), de gerenciamento (SMT), ou se é a permissão. Um delimitador de fim de quadro (ED), e dois símbolos delimitadores TT completam o quadro da permissão.

Nos quadros de dados, os campos DA e SA representam os endereços de origem e destino, seguindo as mesmas regras do padrão IEEE 802. FCS é um campo de 32 bits para detecção de erro através de teste de redundância cíclica, usando um polinômio padrão da ANSI (idêntico ao padrão IEEE 802). O delimitador de fim de quadros ED, para quadros que não são a permissão, é constituído do símbolo T, sendo seguido pelo campo FS, que vai indicar se a estação de destino reconheceu o endereço, se o quadro foi copiado, e se qualquer estação detectou erro no quadro.

Atividades de avaliação

1. Descreva o método de acesso ALOHA.
2. Descreva o método de acesso CSMA/CD.
3. Relacione os tipos de cabeamento Ehernet, suas vantagens e desvantagens e indique o local de aplicação.
4. Para que serve o campo Preâmbulo e Delimitador do quadro Ethernet.
5. Qual a aplicação do Algoritmo Backoff Exponencial no protocolo Ethernet.
6. Quais as diferenças no formato do quadro Fast-Ethernet em relação ao quadro Ethernet?
7. Qual a função de auto-negociação no protocolo Fast-Ethernet?
8. Por que o FDDI não utilizou a codificação Manchester?
9. Qual a forma de controle ao meio empregada no FDDI?
10. Qual a vantagem do anel duplo sobre o anel simples na rede FDDI?

4. Redes Sem Fio

O primeiro conceito de redes sem fio surgiram no início do Século XX a partir das descobertas de aplicações do eletro magnetismo. A rede Aloha no Havaí possibilitou a ligação entre as ilhas relativamente distantes dessa região, pela inviabilidade de uma interconexão cabeada entre as mesmas. Os pesquisadores locais decidiram desenvolver um sistema de comunicação sem fio capaz de transmitir os dados através da camada atmosférica. O caminho entre o transmissor e o receptor é estabelecido através da propagação das informações por meio de ondas eletromagnéticas, sem a utilização de qualquer conexão física. Assim, surgiram as redes sem fio, sistemas de transmissão de dados que podem substituir ou servir como uma extensão às redes tradicionais.

4.1 Introdução

No início da década passada, a utilização de redes sem fio começou a crescer de forma desordenada. Pela facilidade de instalação, muitas pessoas montavam sua própria rede sem fio, resultando em redes pouco confiáveis, com baixas taxas de transmissão e incompatíveis com a maioria dos equipamentos. A fim de uniformizar esse tipo de rede, em 1998, o órgão internacional IEEE (Institute of Electrical and Electronics Engineers) desenvolveu vários padrões para redes sem fio, como por exemplo, o IEEE 802.11.

Juntamente com o IEEE 802.11, outras tecnologias de redes sem fio conhecidas são Bluetooth e IEEE 802.16. O padrão IEEE 802.11 foi especialmente desenvolvido para aplicações de WLANs (Wireless Local Area Networks), isto é, apropriada para criação de redes locais sem fio. O Bluetooth, também conhecido com IEEE 802.15, é utilizado em redes pessoais WPANs (Wireless Personal Area Networks), isto é, redes em ambiente pessoal (uma sala) e para pequenos dispositivos como PDAs (Personal Digital Assistant), telefones celulares, etc. O IEEE 802.16 foi desenvolvido para redes WMANs (Wireless Metropolitan Area Networks), isto é, redes no ambiente metropolitano, para utilização para acesso sem fio no âmbito de uma cidade.

As redes sem fio possuem características intrínsecas que resultam em vantagens e desvantagens sobre as redes cabeadas. Um ponto negativo é que as transmissões estão sujeitas a uma maior probabilidade de erros, devido às interferências do meio. A segurança na transmissão dos dados em redes sem fio é outro fator crítico, pois com um transmissor irradiando os dados através da rede em todas as direções, meio sem fio, torna-se mais complexo impedir a interceptação das informações.

4.1.1 Estação escondida e Estação exposta

Há duas grandes dificuldades próprias das redes sem fio: o problema da estação escondida e o problema da estação exposta. O caso da estação escondida, mostrada na Figura 2.4.1(a), ocorre quando duas estações transmissoras A e C estão fora do alcance uma da outra e resolvem enviar dados para um mesmo receptor B, que está dentro dos limites dos dois transmissores. Isso ocasiona uma colisão no receptor, que não consegue receber nenhuma das duas mensagens.

O problema da estação exposta, mostrada na Figura 2.4.1(b), acontece quando a estação A está trocando informações com qualquer estação e a estação B quer se comunicar com a estação C. Como B está dentro do alcance de A ela deixa de se comunicar com a estação C (fora do alcance de A) por detectar a portadora do canal e verificar que alguma estação dentro da sua área está transmitindo, quando na verdade a transmissão não teria problema algum.

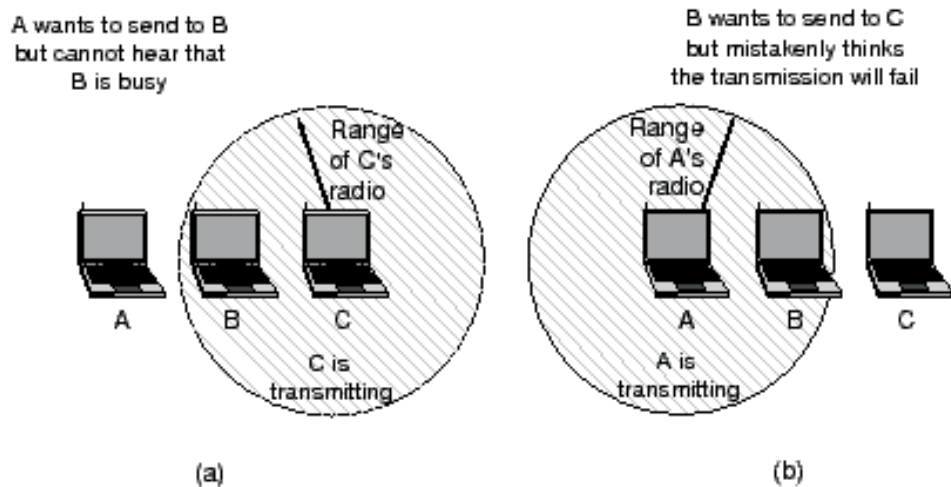



Figura 2.4.1: Estação escondida e exposta.

4.1.2 Redes Ad hoc e Infra-estruturadas

Há duas arquiteturas diferentes em uma rede sem fio: Ad hoc e Infraestruturada.

Rede ad hoc

Nas redes ad hoc, são reunidos computadores para formar uma rede. Como pode ser visto na Figura 2.4.2, não há nenhuma estrutura de comunicação de apoio; não há nenhum ponto fixo; e normalmente toda estação móvel, em uma área restrita, pode estabelecer comunicação ponto-a-ponto entre si. Um exemplo dessa rede é uma reunião empresarial onde executivos compartilham projetos e informações financeiras em seus laptops.

Uma rede Ad hoc tem uma arquitetura simples mas exige uma maior complexidade nos protocolos de controle e sinalização. Como a conectividade da rede depende dos dispositivos móveis, há a possibilidade de haver desconexões momentâneas, em virtude da movimentação dos dispositivos móveis. Isso exige a criação de protocolos de roteamento diferentes das redes fixas. A responsabilidade em encaminhar pacotes pela rede são dos dispositivos móveis. Como a recepção e transmissão de mensagens consome energia é difícil administrar a política de roteamento, particularmente com dispositivos com baixa capacidade de armazenamento de energia.

Figura 2.4.2: Rede Ad hoc.

Rede Infraestruturada

O segundo tipo de rede usado em LANs sem fios é a rede infraestruturada, conforme Figura 2.4.3. Essa arquitetura utiliza dois elementos: as estações móveis e os pontos de acesso (APs). Cada ponto de acesso é responsável pela conexão das estações móveis de sua área de cobertura com a rede fixa. O AP desempenha tarefa importante na coordenação das estações móveis: aceita ou não a inserção de uma nova estação à rede, colhe estatísticas para melhor gerenciamento do canal e ajuda a definir quando uma estação deve ou não ser controlado por outro ponto de acesso. Cada estação está associada a apenas um ponto de acesso em um determinado instante de tempo.

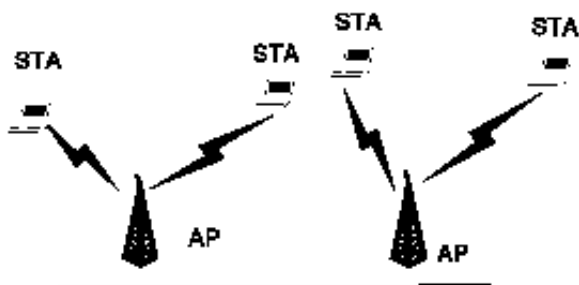
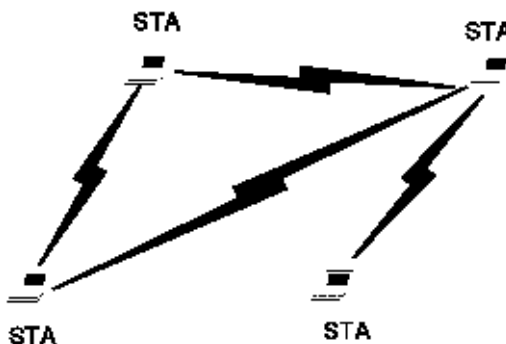



Figura 2.4.3: Rede Infraestruturada.

Em uma rede infraestruturada, todas as estações móveis se comunicam com o AP. O AP provê ambas, a conexão com a rede local fixa, se houver, e a função de transmissão para estação móvel local. Assim, se uma estação móvel precisar se comunicar com outra estação móvel, a comunicação é primeiramente enviada ao AP e então o AP encaminha para a outra estação

móvel. Isto causa duas comunicações que originam e terminam na mesma área, consumindo duas vezes a largura de banda que a mesma comunicação consumiria se fosse enviada diretamente de uma estação móvel a outra. Enquanto isso parece ter um custo significativo, há benefícios: a bufferização do tráfico para uma estação móvel enquanto ela estiver operando em baixa capacidade de energia (dormência).

4.2 Sistemas WLAN

O IEEE (Institute of Electrical and Electronics Engineers) aprovou em 1997, o padrão IEEE 802.11, específico para redes locais sem fio. O escopo deste padrão é desenvolver as especificações das camadas MAC (Medium Access Control Layer) e física (Physical Layer) para prover conectividade sem fio a estações fixas, portáteis ou que estejam se movendo dentro de uma área local.

O grupo 802.11 desenvolveu uma especificação global para equipamentos de rádio e redes operando na banda de frequência de 2,4 GHz, pois esta frequência estava disponível na maioria dos países. Após a consolidação da norma 802.11, vários task groups foram criados para o desenvolvimento de padrões em áreas mais específicas, tais como segurança e qualidade de serviço.

4.2.1 Arquitetura IEEE 802.11

A arquitetura das redes sem fio, mostrada na Figura 2.4.4, é composta por vários elementos que interagem de forma que a mobilidade das estações seja transparente para as camadas superiores. Uma arquitetura WLAN tem como unidade principal uma BSS (Basic Service Set), que é a área de cobertura desse sistema de comunicação, também conhecido como célula, onde várias estações (STA - Stations) membros da BSS podem trocar informações sob o mesmo protocolo MAC. Os membros associados de uma BSS podem se comunicar através de uma unidade central chamada ponto de acesso (AP - Access Point). O padrão IEEE 802.11 pode funcionar em dois tipos de redes: as redes infraestruturadas e as redes ad hoc. Várias estação dentro de uma WLAN pode funcionar também como rede Ad hoc, ou seja, cada estação pode encaminhar os pacotes adiante, assim como um ponto de acesso.

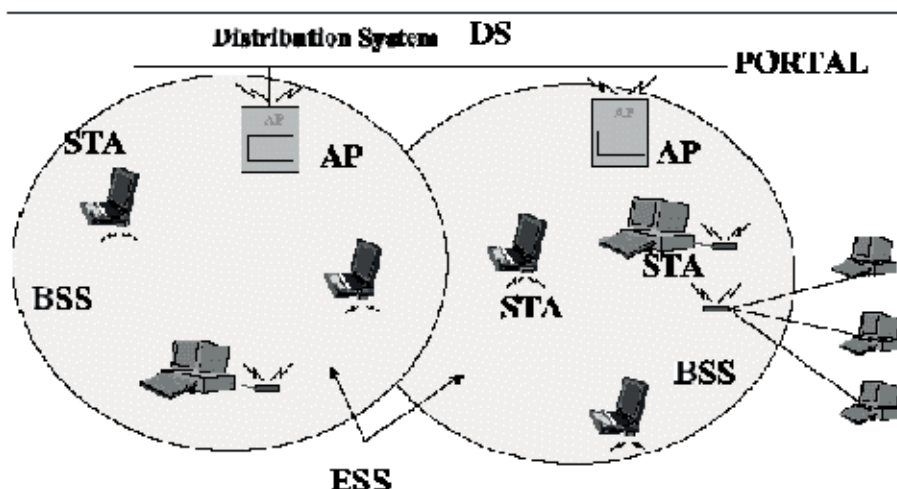



Figura 2.8.4: Arquitetura de uma rede IEEE 802.11.

Duas BSSs podem ser interligadas para obter uma área maior de cobertura através de um sistema de distribuição (DS - Distribution System). A norma 802.11 separa o meio sem fio (WM - Wireless Medium) do meio de sistema de distribuição (DSM - Distribution System Medium) e cada meio lógico é usado para diferentes propósitos. O sistema de distribuição usado para interligar duas ou mais células pode ser tanto o ar, como pode ser uma rede cabeada, daí o porquê de separar o meio sem fio do sistema de distribuição. O componente utilizado para fornecer acesso ao DS é o AP. Combinações de duas ou mais BSSs através de sistemas de distribuição possibilita a criação de redes sem fio de tamanho e complexidade arbitrários, formando a chamada ESS (Extended Service Set).

As STAs de uma rede local sem fio também podem se comunicar umas com as outras sem a presença de um nó que concentra a inteligência do sistema. Essas redes são denominadas Ad hoc network ou IBSS (Independent BSS) e são normalmente estabelecidas por um curto período de tempo em que são necessárias. Essas redes caracterizam-se também pela ausência do sistema de distribuição e, ao contrário das redes infraestruturadas, não podem ser integradas com uma rede cabeada e não utilizam os serviços do sistema de distribuição. A facilidade de instalação e a conectividade direta entre os nós permitem que essas redes sejam estabelecidas rapidamente em qualquer local, o que é uma característica essencial para diversas aplicações.

É possível fazer a conexão entre as rede 802.11 e as redes tradicionais. O elemento que faz essa integração lógica entre os dois tipos de redes é chamado de portal. Ele permite que os dados de uma rede cabeada entrem no serviço de distribuição de uma WLAN.

4.2.2 Modulação Spread-Spectrum

O Spread Spectrum (Espalhamento de frequência) é uma técnica de codificação para transmissão digital, bastante resistente a interferência e interceptação, pois transforma o sinal de informação de maneira que ele se assemelhe a um ruído. O ruído possui um espectro achatado e uniforme sem picos coerentes e que podem geralmente ser removidos por filtragem. Por causa dessa característica de se assemelharem a ruídos os sinais Spread Spectrum são difíceis de serem interceptados, demodulados, ou ainda misturados a sinais de banda estreita.

A técnica de codificação do Spread Spectrum modifica o espectro do sinal, espalhando-o de tal forma que o novo espectro possui uma densidade de potência muito menor, mas a mesma potência total. Esta é, então, a primeira importante característica de um sistema de transmissão Spread Spectrum: A largura de banda do sinal transmitido é muito maior do que a largura de banda da informação propriamente dita.

O espalhamento do espectro é feito antes da transmissão, através do uso de um código que independe da sequência de dados. Um mesmo código é usado no receptor, que deve operar em sincronismo com o transmissor para decodificar o sinal recebido e então recuperar a sequência original de dados.

A expansão da largura de banda transmitida se dá devido a inserção desses códigos, chamados "Pseudo Randômicos" ou "Pseudo Ruídos", e minimiza a interferência de outros usuários, pois abaixa a densidade de potência como já dito anteriormente. A operação de decodificação no receptor é que impede a interferência e desvanecimento por múltiplos caminhos. A segunda importante característica do Spread Spectrum, então é: A sequência de pseudo-códigos é que determina o sinal a ser recebido.

Por estas razões de segurança, a modulação Spread Spectrum foi desenvolvida para aplicações militares na época da Segunda Guerra Mundial, onde se fazia extremamente necessária a imunidade à interferência e interceptação dos sinais pelos inimigos. Os primeiros desenvolvimentos visavam melhorar os sistemas de radares, a comunicação e a navegação.

Entretanto, várias aplicações civis surgiram se beneficiando dessas importantes características do Spread Spectrum. Por exemplo, a rejeição de múltiplos caminhos numa estação terrestre de rádio comunicação móvel, ou ainda, comunicações de múltiplo acesso no qual um número de usuários independente compartilha um mesmo canal sem a existência de um mecanismo de sincronização externa.

Existem duas principais técnicas de codificação Spread Spectrum: DSS (Sistema de Sequenciamento Direto), Frequency Hopping (Salto de frequência).

DSSS - Direct Sequence Spread Spectrum

Nos sistemas de sequenciamento direto (DSSS), a fase da portadora do sinal transmitido é variada de acordo com a sequência de pseudo-ruídos. Isto é geralmente conseguido, multiplicando-se o sinal digital com uma sequência de "chips" (onde chip é o período de uma sequência de pseudo-ruídos). Como a sequência de chips varia a uma taxa muito mais alta que o sinal digital, a largura de banda é significativamente expandida em relação à do sinal que efetivamente contém a informação. No receptor, a informação é recuperada remultiplicando o sinal a uma réplica da sequência de pseudo-ruídos, gerada localmente. Isto efetivamente comprime o sinal de volta à sua largura de banda original, entretanto no processo de multiplicação do sinal que acontece no receptor alguma interferência é espalhada junto ao sinal, mas é facilmente removida com filtragem.

No sequenciamento direto, o que determina o espalhamento do espectro é a taxa de variação da sequência de pseudo-ruídos (chips) por bits de informação. Quanto maior for a sequência de pseudo-ruídos, mais difícil de ser detectado e interceptado será o sinal, porém uma maior tecnologia é exigida dos equipamentos de detecção e correlação.

FHSS - Frequency Hopping Spread Spectrum

Nos sistemas de Frequency Hopping (Salto de frequência), a frequência da portadora do sinal transmitido é variada (ou saltada) de acordo com a sequência de pseudo-ruídos. A ordem das frequências selecionadas pelo transmissor é pré-determinada pela sequência de códigos, e o receptor rastreia essas variações de frequência e produz um sinal de FI frequência intermediária constante. A interferência não é rastreada entretanto pode ocasionalmente estar incluída no sinal de FI. Podem ser do tipo rápido (Fast Frequency Hopping) ou lento (Slow Frequency Hopping)

4.2.3 Camada Física (PHY)

A camada física (PHY) define as características mecânicas, elétricas, funcionais e procedurais para ativar, manter, e desativar conexões físicas, que se destinam a transmitir bits entre entidades do nível de enlace. As características mecânicas definem, por exemplo, o tamanho e a forma dos conectores, pinos, cabos etc., que compõem um circuito de transmissão. As características elétricas especificam os valores dos sinais elétricos (níveis de voltagem e corrente) usados para representar bits, o tempo entre mudanças desses valores (intervalo de sinalização) etc. As características elétricas determinam as taxas de transmissão e distâncias que podem ser atingidas. Já as características funcionais definem o significado dos sinais transmitidos nas interfaces do nível físico. As características

procedurais especificam combinações e sequências de sinais que devem ocorrer para que uma interface do nível físico cumpra o seu papel de transmitir bits.

A PHY, situa-se ao fundo da pilha do modelo OSI, conforme pode ser visto na Figura 2.4.5. A PHY é a interface entre a subcamada de controle de acesso ao meio (MAC) e o meio sem fio, transmitindo e recebendo quadros de dados sobre o meio sem fio compartilhado.

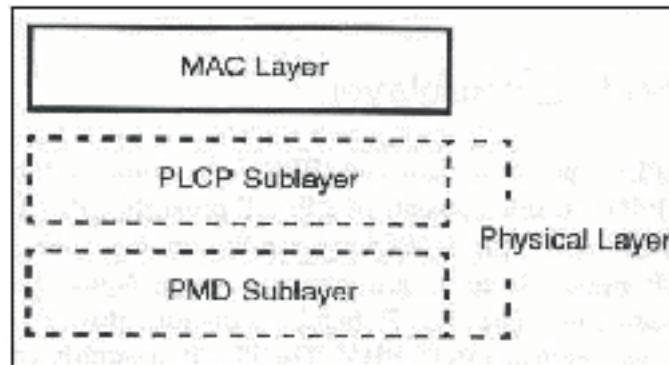



Figura 2.4.5: Representação da Camada Física (PHY).

A PHY provê três níveis de funcionalidade. A primeira, provê a troca de quadros entre o MAC e a PHY, sob o controle da subcamada de procedimento de convergência da camada física (PLCP). A segunda, a PHY utilizada o sinal da portadora e modulação de espalhamento espectral para transmitir quadros de dados sobre o meio, controlada pela subcamada de dependência do meio físico (PMD). Na terceira funcionalidade, a PHY fornece uma indicação da portadora visando a verificação da atividade do meio.

Como meio de transmissão, as redes locais sem fio possuem duas formas de fazê-lo: por canais de radiofrequência ou raios infravermelhos.

As redes que empregam raios infravermelhos são compostos de equipamentos mais simples, haja vista referida rede necessitar apenas a detecção da amplitude de sinais ópticos. Redes que utilizam os raios infravermelhos como meio de transmissão são tidos como sistemas de baixo custo e não possuem restrições dos órgãos regulamentadores.

As redes de radiofrequência apresentam um cenário oposto as de raios infravermelhos. A tecnologia de radiofrequência na qual WLANs são baseadas é conhecida como modulação de espalhamento espectral e tem suas raízes na atividade militar datada da Segunda Guerra Mundial. Entre as vantagens que podem ser elencadas no uso da tecnologia de espalhamento espectral podemos citar: a segurança inerente as transmissões, resistência para interferência ocasionais e intencionais, redundância, resistência para multicaminhos (multipath) e efeito fading.

O espalhamento do sinal pela banda é realizado por um código independente dos dados. Para o receptor recuperar o sinal original, a recepção deve ser sincronizada com o transmissor através deste código. Um dos parâmetros-chave desta técnica reside nos número de formatos de sinais ortogonais que podem ser utilizados para a transmissão de dados. Sinais ortogonais são os sinais empregados em um formato para comunicação que não podem ser detectados por processadores do outro formato. A multiplicidade de formatos de sinal permite o acesso múltiplo de comunicação simultaneamente. Dois pontos que se comunicam, possuem o mesmo código, de maneira que o receptor possa recuperar o sinal transmitido, apesar de outras transmissões estarem sendo feitas ao mesmo tempo.

Como resultado, sistemas que utilizam espalhamento espectral podem coexistir com outros sistemas de rádio, sem causar transtornos ou perturbações às atividades dos demais. O efeito imediato deste comportamento é que estes sistemas podem ser operados sem a necessidades de licença, e isso fez a modulação de espalhamento espectral ser a tecnologia escolhida para WLAN.

São apresentados 3 (três) padrões na camada PHY como técnicas de transmissão sem fio: Espalhamento Espectral por sequência Direta (DSSS - Direct Sequence Spread Spectrum), Espalhamento Espectral por Faltos de frequência (FHSS - Frecuency Hopping Spread Spectrum) e Infravermelho (IR). As referidas técnicas serão abordadas a seguir.

IEEE 802.11b

O IEEE 802.11b é uma extensão do DS-SS 802.11, fornecendo taxas de dados de 5.5 a 11 Mbps, ocupando o mesmo tamanho de banda. Para alcançar taxas de dados altas na mesma banda, é utilizado o quadro de modulação CCK (Complementary Code Keying). Na modulação CCK a entrada de dados são negociados em blocos de 8 bits de uma taxa de 1.375Mhz (8 bits/simbolos x 1.375 MHz = 11Mbps).

IEEE 802.11a

O 802.11b utiliza a frequência de 2.4 GHz, a mesma utilizada por outros padrões de rede sem fio e pelos micro-ondas, todos potenciais causadores de interferência. O 802.11a por sua vez utiliza a frequência de 5 GHz, onde a interferência é menor. Graças à frequência mais alta, o padrão também é quase cinco vezes mais rápido, atingindo 54 megabits.

Outra vantagem é que o 802.11a permite um total de 8 canais simultâneos, contra apenas 3 canais no 802.11b. Isso permite que mais pontos de acesso sejam utilizados no mesmo ambiente, sem que haja perda de desempenho.

O grande problema é que o padrão também é caro, por isso sua adoção

ainda é lenta. Além disso, por utilizarem uma frequência mais alta, os transmissores 8021.11a também possuem um alcance mais curto, teoricamente metade do alcance dos transmissores 802.11b, o que torna necessário usar mais pontos de acesso para cobrir a mesma área, o que contribui para aumentar ainda mais os custos. Outro problema é que as antenas 2.4 GHz são incompatíveis com as de 5 GHz, assim, atualizar uma rede 802.11b para 802.11a exige a toca de antenas e redistribuição de APs para funcionar, aumentando ainda mais o custo.

O 802.11a utiliza a modulação OFDM (Orthogonal Frequency Division Multiplexing), também conhecido como modulador multicarrier, utilizado por portadores múltiplos de sinais de diferentes fases para enviar bits sobre cada canal. As taxas de dados possíveis para esta especificação são 6, 9, 12, 18, 24, 36, 48 e 54 Mbps.

IEEE 802.11g

Este é um padrão recentemente aprovado pelo IEEE, que é capaz de transmitir dados a 54 megabits, assim como o 802.11a.

A principal diferença é que este padrão utiliza a mesma faixa de frequência do 802.11b atual: 2.4 GHz. Isso permite que os dois padrões sejam compatíveis. A ideia é que você possa montar uma rede 802.11b agora e mais pra frente adicionar placas e pontos de acesso 802.11g, mantendo os componentes antigos e a distribuição dos APs, assim como hoje em dia temos liberdade para adicionar placas e hubs de 100 megabits a uma rede já existente de 10 megabits.

A velocidade de transferência nas redes mistas pode ou ser de 54 Mbps ao serem feitas transferências entre pontos 802.11g e de 11 Mbps quando um dos pontos 801.11b estiver envolvido, ou então ser de 11 megabits em toda a rede, dependendo dos componentes que forem utilizados. Esta é uma grande vantagem sobre o 802.11a, que também transmite a 54 megabits, mas é incompatível com os outros dois padrões.

4.2.4 Camada de Acesso ao Meio (MAC)

O grupo de trabalho IEEE 802.11 foi formado como o objetivo de especificar um padrão internacional para redes locais sem fio visando satisfazer as seguintes necessidades: fazer a interconexão com o sistemas existentes e zelar pela produtividade do usuário final estabelecendo o tempo de resposta nas redes sem fio como algo aceitável. Para tanto, a subcamada de controle de acesso ao meio, doravante denominada MAC, deve aparecer para a camada LLC (Logic Link Control) e superiores como qualquer outra rede 802.x.

Para que isto seja factível, o padrão 802.11 descreveu:

- Funções e serviços exigidos por dispositivos nas redes 802.11, bem como os aspectos referentes a mobilidade;
- Serviços para provimento de segurança e privacidade;
- Procedimentos suportando a entrega dos dados limitadas no tempo e assíncrona.

Sendo assim, este tópico visa descrever as funcionalidades da MAC, aspectos relevantes relativos a mobilidade, métodos de controle de acesso, formato dos quadros nas redes sem fio, privacidade e segurança objetivando formação conceitual sobre este importante elemento coberto pelas especificações IEEE 802.11.

Funcionalidades da MAC

A MAC, especificada pelo IEEE 802.11 para controle de acesso ao meio, fornece as funcionalidades requeridas para provimento de mecanismo de entrega confiável dos dados dos usuários em um meio sem fio, hostil e não confiável.

A primeira funcionalidade da MAC é prover um serviço de entrega de dados seguro aos usuários desta camada. Através de um protocolo de troca de quadro, ao nível de MAC, o IEEE 802.11 MAC aprimora significativamente a entrega confiável dos dados em um meio sem fio, se comparada a WLANs anteriores ao padrão.

A segunda funcionalidade é o correto controle de acesso em um meio sem fio compartilhado. Ela desenvolve esta função através de dois mecanismos de acesso distintos: o mecanismo de acesso básico, chamado de função de coordenação distribuída (DCF - Distributed Coordination Function) e o mecanismo de acesso controlado centralizadamente, denominado função de coordenação pontual (PCF - Point Coordination Function).

A terceira funcionalidade é proteger os dados que são entregues. Uma WLAN não pode estar contida em uma área física restrita, na maioria dos casos. A camada MAC do IEEE 802.11 provê um serviço de privacidade chamado Wired Equivalent Privacy (WEP) que codifica os dados para enviá-los sobre um meio sem fios. O nível de criptografia escolhido se aproxima ao nível de proteção dos dados ao de uma rede fixa, onde é possível controlar o acesso físico, prevenindo conexões não autorizadas.

Protocolo MAC do 802.11

O IEEE 802.11 MAC implementa um protocolo para troca de mensagens que permite a fonte do quadro determinar quando um quadro foi recebido com sucesso pelo destino, conforme mostrado na Figura 2.4.6.

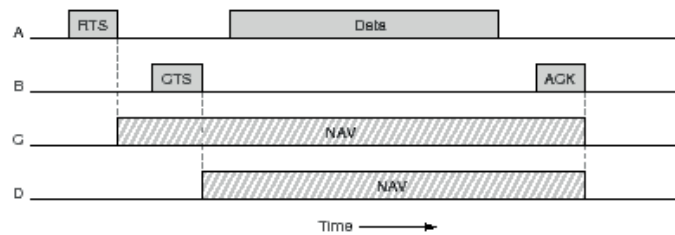



Figura 2.4.6: Funcionamento do CSMA/CA.

A protocolo de troca de quadros da MAC encaminha este problema acrescentando dois quadros. Estes quadros são: um quadro RTS (Request to Send) e um quadro CTS (Clear to Send). A fonte envia um RTS para o destino. Este pacote contém o tamanho do quadro a ser transmitido. Os nodos que ouvem o quadro RTS e não transmitem por um período igual a transmissão de um quadro de resposta pelo destino. O destino devolve um CTS para a origem, que também informa o tamanho do quadro a ser recebido. Os nós "ouvem" o quadro CTS e não transmitem por um período igual ao necessário para a transmissão do quadro pela fonte. Se o quadro é corretamente recebido pelo destino, o destino retorna um ACK (acknowledgement), completando o protocolo de troca de quadro. Dependendo da configuração de uma estação e suas condições locais, a estação pode escolher quando usar os quadros RTS e CTS.

As trocas de quadros são uma unidade atômica do protocolo MAC. Elas não podem ser interrompidos pelas transmissões de outras estações. Se a troca de quadros falhar em qualquer ponto, o estado da troca e a informação transportada por cada quadro permitem que estações que tenham recebidos estes quadros recuperem e tornem a controlar o meio em um período de tempo mínimo. Uma estação no ambiente da estação fonte receberá o quadro RTS e aguardará para enviar qualquer transmissão até receber um quadro RTS de aviso. Se o quadro de aviso não for detectado, a estação pode usar o médio. Similarmente, uma estação no ambiente da estação de destino receberá o quadro CTS e aguardará para enviar qualquer transmissão até receber um quadro ACK. Se o quadro ACK não for detectado, a estação pode usar o meio.

Caso ocorra, na estação fonte, uma falha no protocolo de troca de quadro, ocorrerá uma retransmissão de quadro. Isto é tratado como uma colisão e a regra para agendamento da retransmissão será abordada em seguida, no que se refere ao mecanismo de acesso básico. Para prevenir a MAC de monopolizar tentando entregar um único quadro, existem contadores e timers limitando o tempo de vida de um quadro.

Confirmação de Recebimento no Nível MAC

A camada MAC realiza detecção de colisão esperando a recepção de uma confirmação (acknowledge) de qualquer fragmento transmitido (Pacotes que tem mais que um destino, tais como multicast, não são confirmado).

Protocolos típicos de LANs usam pacotes com várias centenas de bytes (o pacote ethernet mais comprido pode chegar a 1518 bytes). Existem diversas razões porque é preferível usar pacotes menores em um ambiente sem fio.

Entretanto, não faz sentido introduzir um novo protocolo de LAN que não possa tratar com pacotes de 1518 bytes que são usados na Ethernet. Assim, decidiu-se solucionar o problema adicionando um mecanismo de fragmentação e remontagem simples na camada MAC.

O mecanismo é um simples algoritmo de "Pára-e-Espera", onde a estação transmissora não tem permissão de transmitir um novo fragmento até uma alternativas abaixo acontecer:

1. Receber um ACK para o fragmento enviado, ou
2. Decidir que o fragmento foi retransmitido muitas vezes e descarta todo o quadro.

Deve ser levado em conta que o padrão permite que a estação transmita para um endereço diferente entre retransmissões de um dado fragmento. Isso é particularmente útil quando um AP tem vários pacotes saindo para diferentes destinos e um deles não responde.

Espaços Inter-Frame

O padrão IEEE 802.11 define 4 tipos de espaços inter frame que são usados para prover controle de acesso ao meio. A Figura 2.4.7 mostra um diagrama de todos os espaços inter-frame, explicados a seguir:

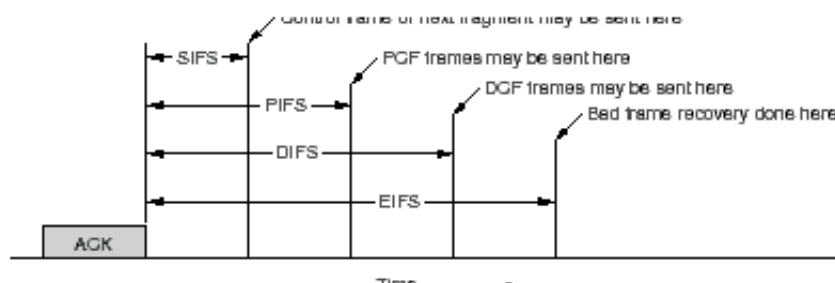



Figura 2.4.7: Espaçamento entre quadros 802.11.

SIFS

Short Inter Frame Space é usado para separar transmissões pertencentes a um único diálogo e é o espaço inter-frame mínimo. Há sempre, pelo

menos, uma estação transmitindo, consequentemente tendo prioridade sobre todas as outras estações. Este valor é um valor fixo para PHY e é calculado de tal forma que a estação transmissora seja capaz de retornar ao modo de recepção e ser capaz de decodificar o pacote recebido. Na 802.11 PHY este valor é de 28 microsegundos.

PIFS

Point Coordination Inter Frame Space é usado pelo Access Point (AP), para ganhar acesso ao meio antes de qualquer outra estação. Este valor é o SIFS mais um slot de tempo. Este valor é de 78 microsegundos.

DIFS

Distributed Inter Frame Space é o Espaço Inter-frame usado por uma estação que deseja iniciar uma nova transmissão, sendo calculada como PIFS mais um slot de tempo. Este valor é 128 microsegundos.

EIFS

Extended Inter Frame Space é o Espaço Inter-frame mais longo usado pela estação que recebeu um pacote que ela não conseguiu entender. Isto é necessário para prevenir a estação (que poderia não entender a informação de duração para o Virtual Carrier Sense) de colidir com um futuro pacote pertencente ao diálogo atual.

Algoritmo Backoff Exponencial

Backoff é um método usado para resolver a disputa entre estações que desejam acessar o meio. O método exige que cada estação escolha um número randômico entre 0 (zero) e um outro número determinado e espera por este número de slots de tempo antes de acessar o meio, sempre conferindo se uma estação diferente acessou o meio antes. Em virtude dessa pré-seleção de slot, o MAC do 802.11 é chamado CSMA/CA (Collision Avoidance). Mostramos na Figura 2.4.8 o diagrama de tempo do CSMA/CA.

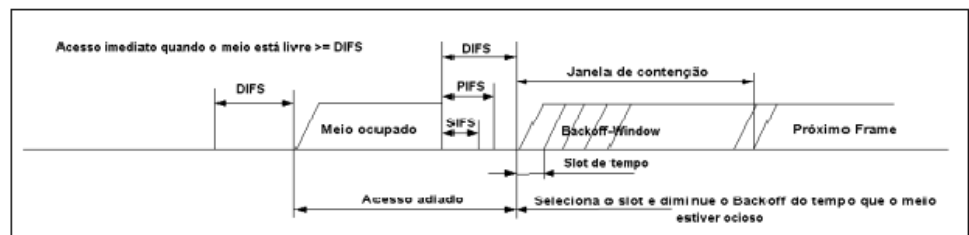



Figura 2.4.8: Diagrama de tempo do CSMA/CA.

O slot de tempo é definido de uma tal maneira que uma estação sempre é capaz de determinar se a outra estação acessou o meio no início do slot anterior. Isto reduz a probabilidade de colisão pela metade. Backoff Exponencial significa que cada vez que a estação escolher um slot e ocorrer uma colisão, ela aumentará o número máximo para a seleção randômica exponencialmente.

No padrão IEEE 802.11 o algoritmo Backoff Exponential deve ser executado nos seguintes casos:

1. Quando uma estação escuta o meio antes da primeira transmissão de um pacote e o meio está ocupado;
2. Após cada retransmissão, e
3. Após uma transmissão bem sucedida.

O único caso em que este mecanismo não é usado é quando a estação decide transmitir um novo pacote e o meio está livre por mais que DIFS.

Formatos e Tipos de Quadros

O padrão IEEE 802.11, especifica três principais tipos de quadros:

Quadros de Dados

são usados para transmissão de dados

Quadros de Controle

são usados para controlar o acesso ao meio (por exemplo RTS, CTS e ACK)

Quadros de Gerenciamento

são transmitidos de maneira semelhante aos quadros de dados para troca de informação de gerenciamento, mas não são encaminhados para as camadas superiores.

Cada tipo de quadro é subdividido em subtipos diferentes de acordo com a sua função específica. Todos os quadros especificados pelo IEEE 802.11, conforme a Figura 2.4.9, são compostos pelos seguintes elementos:

Figura 2.4.9: Formato de um quadro genérico do 802.11.

Preâmbulo

Indica o início da transmissão do quadro, semelhante ao quadro Ethernet 802.3.

Cabeçalho PLCP

O cabeçalho PLCP é sempre transmitido em 1 Mbits/s e contém informação lógica usada pela camada física para decodificar o quadro. Ele consiste de:

Tamanho da palavra PLCP_PDU

Representa o número de bytes contido no pacote. Isto é útil para a camada física detectar corretamente o fim do pacote.

Campo de Sinalização do PLCP

Contém somente informação de taxa, codificada em 0,5 Mbps de aumento de 1 Mbits/s até 4.5 Mbits/s.

MAC Data

Dados da camada MAC

CRC

Campo de checagem de erro do cabeçalho, que é um erro CRC de 16 bits.

Quadro MAC

A Figura 2.4.10 representa o formato geral de um quadro MAC.

Figura 2.4.10: Formato de um quadro MAC 802.11.

Frame Control

Campo de controle de quadro, descrito em seguida.

Duração

Este campo tem dois significados dependendo do tipo de quadro: Em

mensagens de polling para economia de energia ele é o ID da estação Em todos os outros quadros ele é o valor da quantidade de tempo usado para o cálculo do Net Allocation Vectors (NAV).

Campos de Endereços

um quadro pode conter até 4 endereços dependendo dos bits ToDS e FromDS definidos no campo de controle.

Endereço-1

é sempre o endereço do receptor (isto é, a estação BSS que é o receptor imediato deste pacote). Se ToDS está setado, ele é o endereço do AP, se ToDS não está setado então é o endereço da estação final.

Endereço-2

é sempre o endereço do transmissor (isto é, a estação que está fisicamente transmitindo o pacote). Se FromDS está setado, ele é o endereço do AP, se não está setado então é o endereço da estação.

Endereço-3

em muitos casos os endereços ficam perdidos. Em um quadro com FromDS setado com 1, Endereço-3 é o endereço fonte original, se o quadro tem o ToDS setado então o Endereço-3 é o endereço destino.

Sequência

O campo Controle de sequência é usado para representar a ordem de diferentes fragmentos pertencentes ao mesmo quadro e reconhecer pacotes duplicados. Ele consiste de dois subcampos, Número do Fragmento e sequência do Fragmento, que definem o quadro número do fragmento no quadro.

CRC

O CRC é um campo de 32 bits que contém um Check de Redundância Cíclica de 32 bits.

O campo de controle de quadro (Frame Control), mostrado na parte inferior da Figura 8.10, define o modo de funcionamento e o significado dos diversos campos.

Versão do Protocolo

este campo consiste de 2 bits que são invariáveis em tamanho e mantém-se através das seguidas versões do padrão 802.11 e deverá ser usado em possíveis versões futuras. Na versão atual do padrão IEEE 802.11 o valor é fixo em 0.

Tipo e Subtipo

estes 6 bits definem o tipo e o subtipo do quadro, conforme pode ser visto na tabela .

ToDS

este bit é setado para 1 quando o quadro é endereçado para o AP encaminhá-lo para o DS (incluindo o caso onde a estação destino está no mesmo BSS e o AP reencaminha o quadro). O bit é setado para 0 em todos os outros quadros. A tabela mostra os diversos significados dos campos de endereço comforme ToDS e FromDS.

FromDS

este bit é setado para 1 quando o quadro é recebido do Distribution System (DS).

MF

More Fragments - este bit é setado para 1 quando há mais fragmentos pertencentes ao mesmo quadro seguinte ao fragmento atual.

Retry

este bit indica que este fragmento é uma retransmissão de um fragmento transmitido previamente. Isto é usado pela estação receptora para reconhecer transmissões duplicadas de quadros que podem ocorrer quando um pacote ACK é perdido.

PWR

Power Management: este bit indica o modo de gerenciamento de energia que a estação estará após a transmissão deste quadro. Isto é usado pelas estações que estão mudando o estado de economia de energia para ativa ou vice-versa.

More

Mais Dados: este bit é usado para gerenciamento de energia pelo AP para indicar que há mais quadros bufferizados para esta estação. A estação pode decidir usar esta informação para continuar o processo de polling ou mesmo mudar para o modo ativo.

W

WEP: este bit indica que o corpo do quadro está criptografado de acordo com o algoritmo WEP.

O

Ordem: este bit indica que este quadro está sendo enviado usando a classe de serviço Strictly-Ordered.

A tabela 2.4.1 sumariza o significado das mensagem de acordo com os valores dos campos Tipo e Subtipo.

Tabela 2.4.1

SIGNIFICADO DOS CAMPOS TIPOS E SUBTIPOS			
Valor do Tipo	**Descrição do Tipo**	**Valor do Subtipo**	**Descrição do Subtipo**
b3 b2		b7 b6 b5 b4	
00	Gerenciamento	0000	Association Request
00	Gerenciamento	0001	Association Response
00	Gerenciamento	0010	Association Request
00	Gerenciamento	0011	Reassociation Response
00	Gerenciamento	0100	Probe Request
00	Gerenciamento	0101	Probe Response
00	Gerenciamento	0110-0111	Reserved
00	Gerenciamento	1000	Beacon
00	Gerenciamento	1001	ATIM
00	Gerenciamento	1010	Disassociation
00	Gerenciamento	1011	Authentication
00	Gerenciamento	1100	Deauthentication
00	Gerenciamento	1101-1111	Reserved
01	Controle	0000-0001	Reserved
01	Controle	1010	PS-Poll
01	Controle	1011	RTS
01	Controle	1100	CTS
01	Controle	1101	ACK
01	Controle	1110	CF End
01	Controle	1111	CF End + CD-ACK
10	Dados	0000	Data
10	Dados	0001	Data + CF-ACK
10	Dados	0010	Data + CF-Poll
10	Dados	0011	Data + CF-ACK + CF-Poll
10	Dados	0100	Null Fuction (no data)
10	Dados	0101	CF-ACK (no data)
10	Dados	0110	CF-Poll (no data)
10	Dados	0111	CF-ACK + CF-Poll (no data)
10	Dados	1000-1111	Reserved
10	Dados	0000-1111	Reserved

A tabela 2.4.2 sumariza o uso de diferentes endereços de acordo com os bits setados para ToDS e FromDS.

Tabela 2.4.2

SIGNIFICADO DOS ENDEREÇOS CONFORME CAMPOS TODS E FROMDS					
ToDS	FromDS	Endereço-1	Endereço-2	Endereço-3	Endereço-4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	AS	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Atividades de avaliação

1. Defina uma rede sem fio infraestruturada e ad hoc, quais são suas características principais?
2. Quais as vantagens de um sistema de rede local sem fio na frequência de 5,7 Ghz em relação ao sistema em 2,4 Ghz? E quais as desvantagens?
3. Explique o funcionamento dos intervalos interframe do protocolo IEEE 802.11. Por que eles são diferentes?

Síntese do capítulo

Nesta unidade apresentamos as arquitetura de vários protocolos de comunicação usados em Redes de Computadores. Iniciamos com conceitos gerais de uma camada de Enlace genérica com seus princípios. Depois apresentamos detalhes da camada de enlace com vários exemplos de protocolos para redes de longa distância (WAN), redes locais (LAN) e, finalmente, redes locais sem fio (WLAN).

Leituras, filmes e sites

Sites

Página da Wikipedia com vasto material sobre Camada de Enlace (em português)

http://pt.wikipedia.org/wiki/Camada_de_ligação_de_dados

Apresentação de vários protocolos de redes de computadores (em inglês)

http://www.protocols.com/

Explicação de vários protocolos LAN, WAN e WLAN (em inglês)

http://en.wikipedia.org/wiki/Computer_networking

Referências

ANDREW S. TANENBAUM **Redes de Computadores** 4ª Ed. Editora: Campus, 2004. Livro de referência clássica com mais de 30 anos desde a primeira edição, proporcionando ao estudante uma visão histórica das arquitetura e protocolos de redes de computadores. São quase 1.000 páginas de texto com descrição detalhada dos sistemas e protocolos, além disso, o autor tem um ótimo senso de humor tornando a leitura muito agradável.

LARRY L. PETERSON & BRUCE S. DAVIE **Redes de Computadores: uma Abordagem de Sistemas**. 3ª Ed. Editora: Campus, 2004. Livro texto, tratando não apenas da descrição dos sistemas de redes de computadores mas fornecendo uma explicação do funcionamento. É um livro introdutório mas completo e coeso. Essa edição apresenta assuntos atuais como IPv6, redes peer-to-peer e redes móveis.

KEITH W. ROSS & JAMES F. KUROSE. **Redes de Computadores e a Internet: Uma Abordagem Top-down.** 3ª Ed. Editora: Addison-Wesley, 2006. O grande diferencial desse livro, desde sua primeira edição, é a proposta inovadora da visão top-down no estudo dos conceitos de redes de computadores, isto é, começando na camada de aplicação e descendo até a camada física. Mas independentemente da visão adotada, é um excelente livro com conteúdo detalhado e leitura agradável. Quem preferir a visão tradicional, bottom-up, pode começar pelo último capítulo.

THEODORE S. RAPPAPORT. **Comunicações Sem Fio: Princípios e Prática.** 2ª Ed. Editora: Prentice-Hall, 2009. Esse livro apresenta de maneira didática conceitos técnicos, projetos e implementação de sistemas de comunicação sem fio. São apresentados detalhes de redes de telefonia celular, 3G, Wimax, Wi-fi, Bluetooth, dentre outros. O livro foca em redes sem fio, portanto é necessário um conhecimento prévio de redes de computadores geral para facilitar o entendimento.

Capítulo 3

Protocolos Internet

Objetivos

- Nesta unidade vamos apresentar os conceitos básicos dos protocolos Internet. Começamos com os conceitos de um protocolo de rede e o protocolo IP, tanto na versão 4 como na versão 6. Em seguida apresentamos os conceitos de roteamento na Internet e os principais protocolos. Em seguida mostramos os protocolos da camada de transporte, TCP e UDP. Finalmente, apresentamos algumas aplicações Internet como dns,e-mail, http, ftp e telnet.

1. Rede

Se a comunicação ocorresse apenas entre dois pontos, a camada de enlace seria suficiente pois ela possibilita a transmissão de dados sem erro e na taxa adequada ao receptor. Mas a maioria das redes têm ligações que ultrapassam os limites de uma comunicação entre dois pontos, que exige que um pacote viaje através de diversas redes diferentes. O encaminhamento de pacotes através de diversas redes é a função da camada de Rede. A seção 9.1 apresenta as características e funcionalidades da camada de rede. A seção 9.2 mostra o protocolo IP versão 4, a seção 9.3 apresenta o protocolo para teste de conectividade ICMP, a seção 9.4 mostra o protocolo ARP, e finalmente, a seção 9.5 apresenta a nova versão do protocolo IP, a versão 6.

1.1 Funções da camada de Rede

A camada de rede é responsável pelo encaminhamento de pacotes desde sua origem até o destino final, passando por todos os dispositivos intermediários. Enquanto a camada de enlace se preocupa apenas com o envio de pacotes de uma extremidade a outro de um fio, a camada de rede se preocupa em encaminhá-los do remetente ao destinatário. A Figura 3.1.1 apresenta um diagrama com a posição da camada de rede.

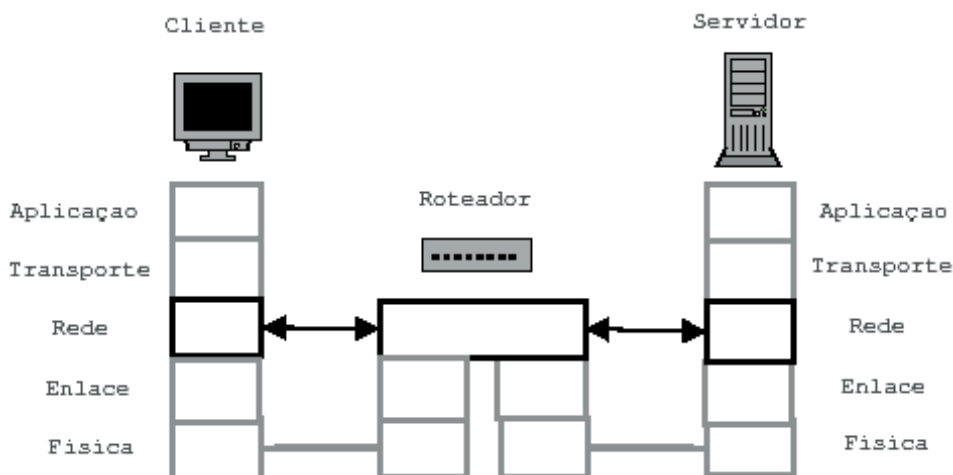



Figura 3.1.1: Diagrama da camada de Rede.

1.2 Protocolo IP

Atualmente o protocolo de rede mais utilizado é, sem dúvida, o protocolo IP, padrão na arquitetura Internet. O protocolo IP é um protocolo datagrama e que realiza expedição de pacotes sem conexão. O protocolo IP tem três características importantes:

1. É o protocolo básico para transferência de dados na Internet. A Internet utiliza vários protocolos de enlace ou físico, dispõe de alguns protocolos de transporte e várias aplicações, porém apenas um protocolo de rede: o IP.
2. A camada IP executa a função de roteamento, escolhendo o caminho para onde os dados serão enviados. O endereçamento IP segue uma estrutura hierárquica.
3. A separação de rede (network) e máquina (host) garante a entrega do pacote ao seu destino e reduz o tamanho das tabelas de roteamento.

1.2.1 Endereçamento na Internet

A Internet é um serviço de comunicação universal porque permite a qualquer equipamento se comunicar com outro qualquer. Para que um sistema ofereça um serviços de comunicação universal é necessário obedecer duas regras:

1. Todos os equipamentos usam um mesmo protocolo de Rede (IP).
2. Cada equipamento tem um endereço único exclusivo, isto é, só existe um determinado endereço IP no mundo.

Assim, na Internet a cada computador é associado um endereço inteiro de 32 bits, chamado endereço IP. A organização de endereços na internet é hierárquico para aumentar a eficiência do roteamento. Um endereço IP define o identificador da rede ao qual o equipamento está conectado e também a identificação desse equipamento nessa rede, que é único.

Para o roteamento entre redes apenas a identificação da rede é importante, e para uma rede apenas a identificação da máquina é importante. A versão atual do protocolo IP utiliza endereços com 32 bits ou 4 bytes e o endereço é representado por quatro números decimais separados por ponto, onde cada número pode assumir um valor de oito bits (0 à 255).

De todos os endereços possíveis em uma rede, foi definido que dois tem aplicação específica e não podem ser escolhidos para identificar uma máquina. O primeiro endereço de máquina, que tem todos os bits 0, identifica a rede. O último endereço, que todos os bits 1, é o endereço de difusão (broadcast), usado para difundir uma mensagem para todos os equipamentos dessa rede. Apresentamos na Figura 3.1.2 um exemplo do esquema de endereçamento na Internet.

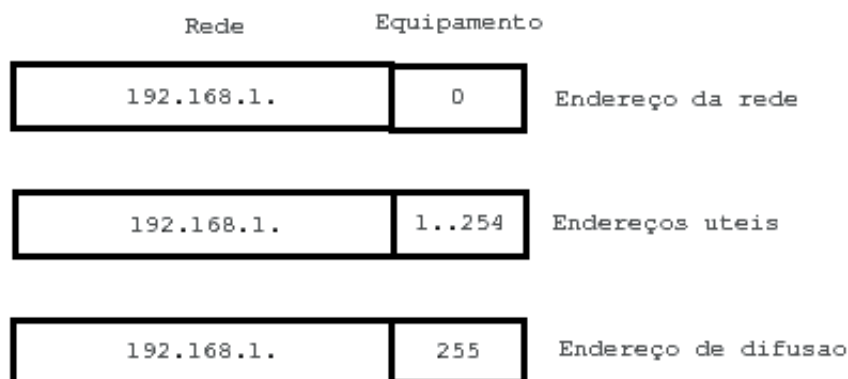



Figura 3.1.2: Esquema de endereçamento na Internet.

Para organizar a utilização destes números foram definidas cinco classes de endereçamento. Cada classe define um campo para endereço da rede e outro para endereço de cada máquina. Para permitir maior flexibilidade os tamanhos de campos são diferentes. As classes são mostradas na Figura 3.1.3.

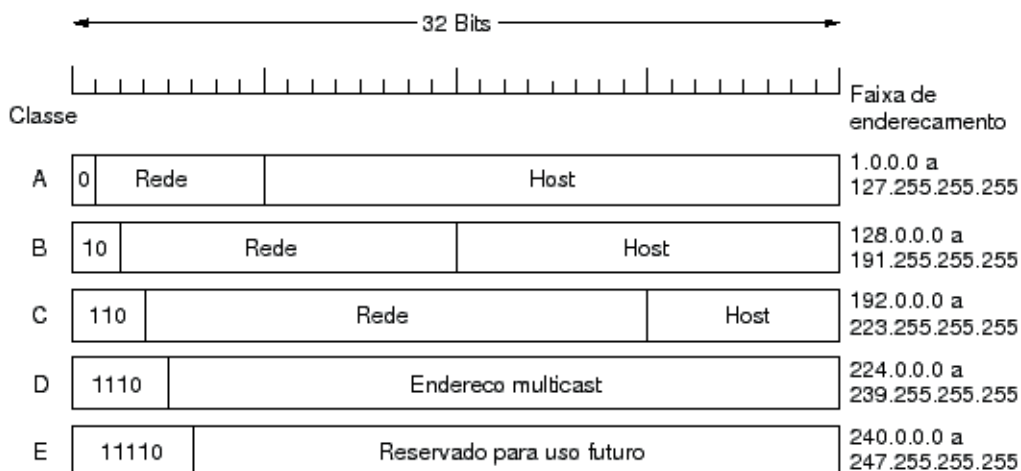



Figura 3.1.3: Divisão de endereços IP por classes.

A organização por classes não é eficiente. É difícil uma organização utilizar toda uma classe A (16 milhões de endereços) e mesmo toda uma classe B (65.536 endereços). Por outro lado, uma classe C (256 endereços) é muito pequena para muitos casos. Para solucionar esse problema foi definida a metodologia CIDR onde podemos agregar várias classes C para formar uma rede maior. Nesse caso é necessário a utilização de uma máscara de rede diferente das classes A, B ou C.

Tabela 3.1.2:

QUANTIDADE DE DISPOSITIVOS POR CLASSES			
Classe	Quant.Redes	Quant.Endereço	Faixa de Endereços
A	128	16 milhões	1.0.0.0 à 127.255.255.255
B	16.384	65.536	128.0.0.0 à 191.255.255.255
C	2 milhões	256	192.0.0.0 à 223.255.255.255
D		268 milhões	224.0.0.0 à 239.255.255.255
E		134 milhões	240.0.0.0 à 247.255.255.255

A organização por classes é um dos motivos da exaustão de endereços IP atualmente e o principal motivo para migração para nova versão IPv6. Atualmente todas as classes A e B estão esgotadas e as classes C disponíveis não são muitas.

1.2.2 Subredes

A utilização da máscara de rede permite outra função importante: dividir uma rede em vários pedaços (subredes) utilizando máscaras apropriadas. Assim, foi possível flexibilizar o conceito de classes, onde a divisão da identificação de rede e máquina ocorre somente a cada 8 bits.

Em uma subrede a identificação de rede e máquina no endereçamento IP pode utilizar qualquer quantidade de bits, e não apenas múltiplos de 8 bits conforme ocorria anteriormente. A máscara identifica em um endereço IP a porção de bits utilizada para identificar a rede e que porção de bits utilizada para máquina.

A máscara é formada por 4 bytes com uma sequência contínua de 1's, seguida de uma sequência de 0's. A porção de bits em 1 identifica os bits utilizados para identificar a rede no endereço e a porção de bits em 0 identifica os bits do endereço que identificam a máquina. Usualmente se representa uma máscara pelo número decimal relativo a cada byte separados por ponto.

Outra forma de representar um máscara é através da quantidade de bits 1 utilizados. Por exemplo a máscara 255.255.255.0, pode ser representada como /24. Este tipo de notação é empregada em protocolos de roteamento mais recentes. A Figura 3.1.4 mostra o esquema de máscara de subrede.

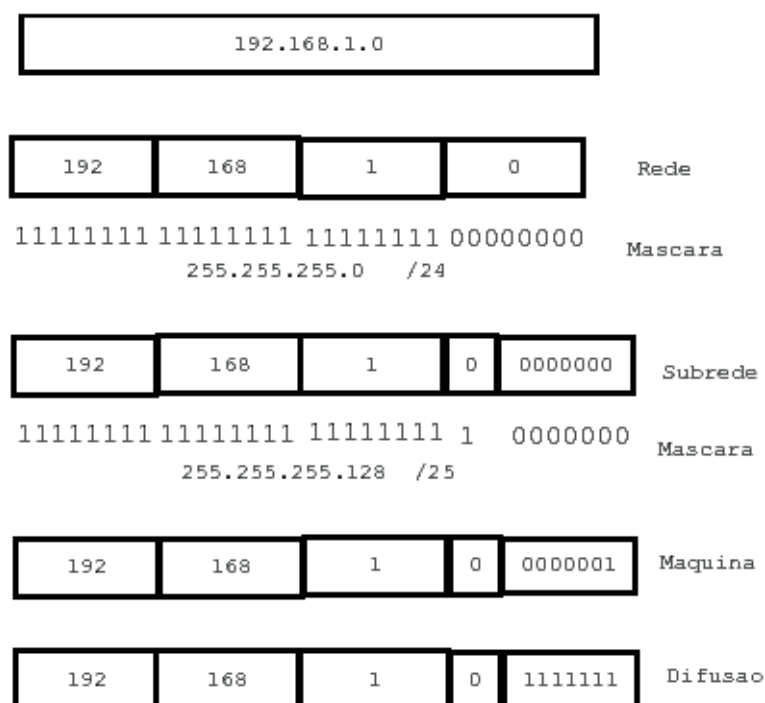



Figura 3.1.4: Máscara de subrede.

A tabela 3.1.2 mostra os valores de máscara utilizados para criar subredes de diversos tamanhos. Ela apresenta o valor da máscara, a quantidade de redes em uma classe C, a quantidade de endereços para cada subrede e a quantidade de endereços úteis.

Tabela 3.1.2

Máscara de subredes				
Máscara	**Máscara(/)**	**Quant.Subredes**	**Quant.Endereço**	**Endereços Úteis**
255.255.255.0	/24	1	256	254
255.255.255.128	/25	2	128	126
255.255.255.192	/26	4	64	62
255.255.255.224	/27	8	32	30
255.255.255.240	/28	16	16	14
255.255.255.248	/29	32	8	6
255.255.255.252	/30	64	4	2

1.2.3 Formato do Datagrama IP

O datagrama IP é a unidade básica de dados no nível IP. Um datagrama está dividido em duas áreas, uma área de cabeçalho e outra de dados.

O cabeçalho contém toda a informação necessária que identificam o conteúdo do datagrama. Na área de dados está encapsulado o pacote do nível superior, ou seja um pacote TCP ou UDP.

O formato geral do datagrama IP é mostrado na Figura 3.1.5.

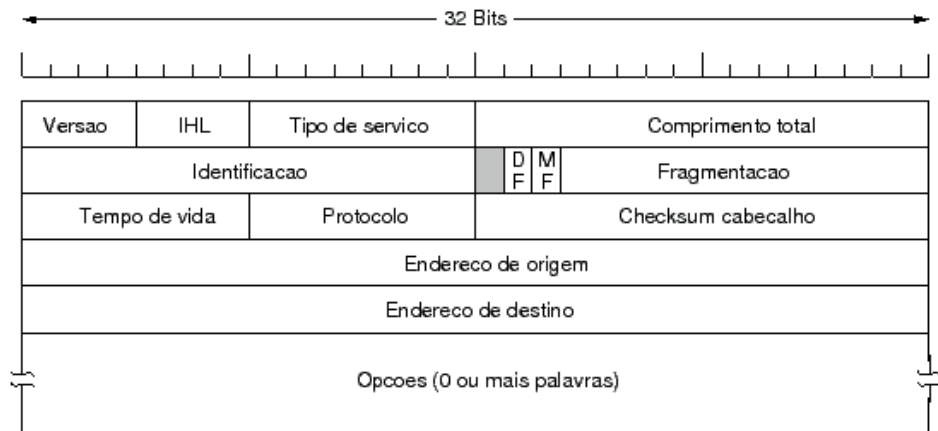



Figura 3.1.5: Cabeçalho do protocolo IP.

O significado dos campos do datagrama IP é o seguinte:

VERSÃO:

versão do protocolo IP que foi usada para criar o datagrama (4bits). Pode ser 4 ou 6.

IHL:

comprimento do cabeçalho, medido em palavras de 32 bits (4 bits)

TIPO DE SERVIÇO:

este campo especifica como o datagrama poderia ser manejado e dividido em cinco subcomandos: Precedence (3 bits) indica precedência de datagramas com valores desde 0 (precedência normal) até 7 (controle da rede), com estes bits permite-se ao transmissor indicar a importância de cada datagrama que ele está enviando.

Bits D,T,R: indicam o tipo de transporte que o datagrama deseja, Baixo Retardo(D), Alta Capacidade de Processamento(T) e Alta Confiabilidade(R).

Não é possível que estes tipos de serviços sempre sejam oferecidos, já que dependem das condições física da rede.

COMPRIMENTO TOTAL:

este campo proporciona o comprimento do datagrama medido em bytes, incluindo cabeçalho e dados.

IDENTIFICAÇÃO, FLAGS e FRAGMENTAÇÃO:

estes três campos controlam a fragmentação e a união dos datagramas.

IDENTIFICAÇÃO:

O campo de identificação contém um único inteiro que identifica o data-

grama, é um campo muito importante porque quando um gateway fragmenta um datagrama, ele copia a maioria dos campos do cabeçalho do datagrama em cada fragmento, então a identificação também deve ser copiada, com o propósito de que o destino saiba quais fragmentos pertencem a quais datagramas. Cada fragmento tem o mesmo formato que um datagrama completo.

FRAGMENTAÇÃO:

especifica o início do datagrama original dos dados que estão sendo transportados no fragmento. É medido em unidades de 8 bytes.

DF:

indica a não fragmentação do pacote (Don't Fragment).

MF

indica que existe um fragmento da mensagem no pacote seguinte (More Fragment).

TTL(Tempo de Vida):

especifica o tempo em segundos que o datagrama está permitido a permanecer no sistema Internet. Gateways e hosts que processam o datagrama devem decrementar o campo TTL cada vez que um datagrama passa por eles e devem removê-lo quando seu tempo expirar. Esse campo serve para evitar que um datagrama transmitido na Internet com endereço errado fique circulando eternamente.

PROTOCOLO:

especifica qual protocolo de alto nível foi usado para criar a mensagem que está sendo transportada na área de dados do datagrama.

CHECKSUM CABEÇALHO:

assegura integridade dos valores do cabeçalho.

ENDEREÇO DE ORIGEM E DESTINO:

especifica o endereço IP de 32 bits do remetente e receptor.

OPÇÕES:

é um campo opcional. Este campo varia em comprimento dependendo de quais opções estão sendo usadas.

1.3 Internet Control Message Protocol (ICMP)

Como IP provê um serviço de expedição de datagramas sem conexão e não confiável, e além disso um datagrama viaja de um gateway a outro até alcançar um gateway que possa expedí-lo diretamente ao host destino; é necessário um mecanismo que emita informações de controle e de erros quando acontecerem problemas na rede. Alguns dos problemas típicos que podem acontecer são:

- Um gateway não pode expedir ou rotear um datagrama
- Um gateway detecta uma condição não usual tal como congestionamento.

O mecanismo de controle que emite mensagens quando acontece algum erro é a função principal do protocolo ICMP.

O ICMP permite aos gateways enviar mensagens de erros ou de controle a outros gateways ou hosts. ICMP provê comunicação entre os software de IP numa máquina e o software de IP numa outra máquina.

ICMP somente reporta condições de erros à fonte original. A fonte deve relatar os erros aos programas de aplicação individuais e tomar ação para corrigir o problema. Uma das mensagens que o ICMP pode enviar é: Destination Unreachable, o qual, por sua vez pode ser dos seguintes tipos:

- Network Unreachable (rede não alcançável)
- Host Unreachable (host não alcançável)
- Port Unreachable (port não alcançável)
- Destination Host Unknown (Host destino desconhecido)
- Destination Network Unknown (rede destino desconhecida)

O aplicativo mais conhecido que usa o protocolo ICMP é o Ping.

1.4 Address Resolution Protocol (ARP)

Como descobrir que endereço Ethernet usar quando você quer conversar com um determinado endereço Internet?

Para solucionar esta questão existe um protocolo específico, chamado ARP. Note que o ARP não é um protocolo IP, isto é, os datagramas ARP não tem cabeçalhos IP.

Suponha que você esteja no sistema 128.6.4.194 e queira conectar o sistema 128.6.4.7. Seu sistema primeiro irá verificar que 128.6.4.7 está na mesma rede, então ele pode conversar diretamente via Ethernet. Então ele irá procurar 128.6.4.7 em sua tabela ARP, para ver se o seu endereço Ethernet já é conhecido. Caso seja conhecido, o sistema irá adicionar um cabeçalho Ethernet, e enviar o pacote.

Mas suponha que este sistema não esteja na tabela ARP. Não há como enviar o pacote, porque você precisa do endereço Ethernet. Então o seu sistema usa o protocolo ARP para enviar uma requisição ARP. Essencialmente uma requisição ARP diz “Eu preciso o endereço Ethernet para 128.6.4.7”.

Todo a rede local escuta requisições ARP. Quando um sistema vê uma requisição ARP para ele mesmo, ele é requisitado a responder. Então 128.6.4.7 verá a requisição e responderá com uma resposta ARP dizendo

como resultado "128.6.4.7 é 8:0:20:1:56:34". (Lembre-se que endereços Ethernet são de 48 bits, o que são 6 bytes).

Seu sistema irá salvar esta informação em sua tabela ARP, então os futuros pacotes para esse mesmo endereço poderão ir diretamente. Muitos sistemas tratam a tabela ARP como uma cache, e limpam suas entradas se estas não forem usadas em um determinado período de tempo.

Note que as requisições ARP devem ser enviadas como "broadcasts". Não há como uma requisição ARP ser enviada diretamente ao sistema correto. Afinal, a razão pela qual a requisição ARP está sendo enviada é que você não conhece o endereço Ethernet.

Então um endereço Ethernet para todas as máquinas é usado, isto é ff:ff:ff:ff:ff:ff. Por convenção, todas as máquinas Ethernet prestam atenção nos pacotes com este endereço. Então cada máquina verifica se a requisição é para o seu próprio endereço. Se for, ela reponde. Se não, ela simplesmente a ignora. (Alguns hosts usam requisições ARP para atualizar seu conhecimento sobre outros hosts da rede, mesmo que a requisição não seja para eles.) Note que pacotes cujo endereço IP indica broadcast (ex: 255.255.255.255 ou 128.6.5.255) também são enviados com um endereço Ethernet de broadcast

1.5 IPv6

O protocolo IP atual apresenta várias deficiências e para resolver isso foi proposto uma nova versão de IP. A versão atual foi denominada como versão 4 e a nova versão do protocolo é 6 (existe uma versão 5 de uso experimental em tempo real). O protocolo é conhecido como IPv6 ou IPng (IP next generation).

O histórico do protocolo, a necessidade de uma nova versão, o novo cabeçalho, a nova forma de endereçamento serão alguns pontos abordados.

1.5.1 Apresentação

A nova versão do protocolo IP foi desenvolvida com alguns objetivos, tendo em mente que deveria ser um passo evolucionário em relação à versão 4, não um passo radicalmente revolucionário. Funções desnecessárias foram removidas; funções que trabalhavam bem foram mantidas; e novas funcionalidades foram acrescentadas.

O novo protocolo IP aumenta o espaço de endereçamento de 32 para 128 bits, suportando mais níveis de hierarquia de endereçamento, um número muito maior de nós endereçáveis, e permitindo a autoconfiguração de nós.

O cabeçalho do protocolo foi simplificado, sendo que alguns campos do cabeçalho da versão 4 foram tirados ou deixados como opcionais, de modo a reduzir o processamento de cabeçalhos tanto quanto não se perceba que o

tamanho dos endereços aumentou, o que poderia aumentar também o tempo de processamento dos cabeçalhos. Enquanto os endereços da versão 6 são 4 vezes maiores que os da versão 4, seu cabeçalho é 2 vezes maior.

A flexibilidade de inclusão de opções no futuro no cabeçalho do IPv6 foi aumentada, devido ao fato de se ter cabeçalhos de extensão que podem ser incluídos. Nesses cabeçalhos estão incluídas também extensões que fornecessem suporte para autenticação, integridade de dados e confidenciabilidade. Essa é uma característica obrigatória em todas as implementações do protocolo.

Uma nova capacidade foi adicionada para permitir que o transmissor de um dado pacote requeira um fluxo especial para ele, como uma qualidade de serviço que não seja a default ou um serviço em tempo real, priorizando aplicações que tem uma transmissão contínua em relação a outras que não tem esse fluxo.

Podemos dizer que o IPv6 consiste de duas partes, o cabeçalho básico e os opcionais.

1.5.2 Histórico

Desde os primórdios da Arpanet quando o procotolo IPv4 foi desenvolvida, o poder de processamento dos computadores cresceu muito e o número de máquinas conectadas à rede cresceu exponencialmente. A versão 4 do IP conseguiu se adaptar à todas as mudanças tornando-se cada vez mais popular. No entanto, uma rede do tamanho da Internet atual e a necessidade de oferecer recursos para aplicações multimídia justificou a criação de uma nova versão do protocolo IP.

Em 1991, o IETF chegou à conclusão de que o crescimento exponencial da rede levaria à exaustão dos endereços IP até o final do ano de 1994. Isso se as tabelas de roteamento não esgotassem a capacidade dos roteadores antes dessa data.

Essa crise foi superada a curto prazo com a adoção do CIDR, que consistia em dar blocos de endereços IP Classe C contíguos a cada região do planeta (Europa, Ásia, etc), e essas regiões dividiriam seus blocos em blocos menores, mas ainda contíguos, até que todas as redes tivessem seus endereços. Com o uso de máscara de rede, os roteadores usavam uma máscara para endereçar todo um bloco de endereços e assim conseguiam diminuir a tabela de roteamento.

Mas o CIDR não seria uma solução duradoura, outra deveria ser projetada a longo prazo e que tivesse uma duração maior. Um novo protocolo precisava ser desenvolvido em substituição ao IPv4. Uma proposta foi a adoção do CLNP, que tem um espaço de 160 bits para endereçamento. Entretanto,

além de não suportar serviços multimídia como desejado, por ser uma solução OSI não foi bem quista por alguns elementos.

Em 1993, o IESG (Internet Engineering Steering Group) criou um grupo de trabalho para uma nova versão do protocolo IP, o IpngWG (IP Next Generation Working Group), com base em alguns objetivos que deveriam ser alcançados. O grupo de trabalho, então, selecionou protocolos "candidatos" para a camada de rede da arquitetura TCP/IP. O vencedor foi o SIPP (Simple Internet Protocol Plus), por diferir menos do IPv4, e ter um plano de transição melhor. Mas uma combinação de aspectos positivos dos três protocolos candidatos foi feita e com isso gerou-se a recomendação para a versão 6 do IP em novembro de 1994.

No entanto apesar da maturidade do protocolo Ipv6 ele foi pouco adotado pelos backbones comerciais. A criação do mecanismo NAT (Network Address Tranlator) possibilitou aumentar o aproveitamento dos endereços Ipv4 existentes, tornando desencessária a utilização do Ipv6 imediatamente. No entanto em 2011 os endereços Ipv4 se exauriram o que torna inevitável a utilização do Ipv6 nas próximas redes. Entretanto a compatibilidade entre ambos os protocolos torna essa adoção transparente para o usuário, sendo necessárias modificações apenas nos backbones.

1.5.3 Objetivos do IPv6

Os objetivos que devem ser alcançados com a nova versão do protocolo IP são:

- Suporte a bilhões de hosts - através da expansão do espaço de endereçamento e uma hierarquia mais versátil;
- Redução da tabela de roteamento; Protocolo passível de expansão, através do uso de cabeçalhos de extensão;
- Simplificação do cabeçalho do protocolo, diminuindo o tempo de processamento na análise dos cabeçalhos, por parte de roteadores e hosts;
- Garantia de mais segurança (autenticação e privacidade) em relaçao à versão atual;
- Criação de um campo que suporte mecanismos de controle de qualidade de serviço, gerando maior sensibilidade ao tipo de serviço, como, por exemplo, serviços de tempo real;
- Permissão de multicasting, através da especificação de escopos de sessões multicasting;
- Melhorias no roteamento, inclusive no que tange a hosts móveis;
- Permissão de máquinas wireless mudarem fisicamente de lugar sem mudança em seus endereços IP;

- Habilitação de máquinas se autoconfigurarem (número IP, servidor de nome...) ao serem ligadas na rede, operação “plug and play”;
- Um novo tipo de endereço chamado anycast, conceitualmente uma “cruz” entre unicast e multicast: esse tipo de endereço identifica um conjunto de nós, onde um pacote enviado para um endereço anycast será entregue a um destes nós;
- Coexistência das duas versões do protocolo por um bom tempo, pois não se pode determinar uma data específica para que todas as máquinas no mundo troquem seus softwares.

1.5.4 Endereçamento IPv6

Tipos de Endereços IPv6

O espaço de endereçamento, que era de 32 bits na versão 4 do IP passa a ser de 128 bits. Assim, enquanto IPv4 suportava 4 bilhões de nós, IPv6 pode endereçar 3,4 × 1038 nós.

IPv6 abandona a idéia de classes de endereços, mas baseia-se em prefixos como IPv4, mudando a função desses prefixos. Eles não mais identificam as diferentes classes de endereços, mas diferentes usos de endereços. A tabela 3.1.3 identifica esses prefixos:

Tabela 3.1.3

Prefixos do IPv6	
Prefixo	**Uso**
0000 0000	reservado (incluindo IPv4)
0000 0001	não usado
0000 001	reservado para OSI NSAP
0000 010	reservado para Novell NetWare IPX
0000 011	não usado
0000 1	não usado
0001	não usado
001	não usado
010	Provider-Based unicast
011	não usado
100	Geographic-Based unicast
101	não usado
110	não usado
1110	não usado
1111 0	não usado
1111 10	não usado
1111 110	não usado
1111 1110	não usado
1111 1110 0	não usado
1111 1110 10	Link Local Use
1111 1110 11	Site Local Use
1111 1111	Multicast

Endereços que começam com 80 zeros são reservados para endereçamento IPv4. Duas variantes são suportadas, identificadas nos 16 bits seguintes, que suportarão que IPv6 trafegue numa estrutura ainda baseada em IPv4 .

Duas porções de endereços são reservadas para encapsulamento de protocolos que não sejam o IP, como OSI NSAP e Novell IPX.

O prefixo Provider-Based identifica provedores de acesso. Esse prefixo permite que empresas que provêm acesso à internet ganhem uma grande parcela do espaço de endereçamento, e a dividam hierarquicamente, como CIDR, como mostra a tabela 3.1.4:

Tabela 3.1.4

Prefixo Provider-Based					
3 bits	n bits	m bits	x bits	y bits	x-y bits
010	REGISTRY ID	PROVIDER ID	SUBSCRIBER ID	SBNET ID	INTERFACE ID

Os primeiros 3 bits do endereço identificam o prefixo. O próximo campo identifica o registro na internet do provedor, identificado no campo seguinte. O provedor pode, então, alocar porções para assinantes. Através do campo SUBSCRIBER ID, os assinantes são identificados naquele provedor. SUBNET ID identifica uma subrede, uma ligação física específica. Pode haver mais de uma subrede na mesma ligação física, mas não pode haver mais de uma ligação física na mesma subrede. o último campo identifica a interface ligada na rede (host). Espera-se que para o campo de registro use-se 5 bits, e para o campo de provedores use-se 3 bytes.

O prefixo Geographic-Based é muito similar ao modelo atual, no qual os provedores não alocam grandes espaços. O prefixo indicaria a posição geográfica da rede, e não a partir de onde ela conectada.

Os endereços de uso local (link e site) são, como o próprio nome diz, para uso local, para que máquinas possam se autoconfigurar ao serem conectadas.

A tabela 3.1.5 mostra o prefixo de link local tem o seguinte formato, sendo o mais indicado para autoconfiguração.

Tabela 3.1.5

Prefixo Link Local		
10 bits	n bits	118-n bits
1111111010	0	INTERFACE ID

A tabela 3.1.6 mostra o formato do prefixo de site local.

Tabela 3.1.6

Prefixo Site Local			
10 bits	n bits	m bits	118-n-m bits
1111111011	0	SUBNET ID	INTERFACE ID

Para ambos os tipos INTERFACE ID deve ser único por interface, não podendo se repetir. O campo SUBNET identifica uma subrede dentro desse domínio. O uso desse tipo de endereçamento é útil para a construção de intranets, onde se pode construir uma rede baseada na arquitetura TCP/IP sem se ter endereços alocados. A vantagem desse tipo de endereçamento é que enquanto uma rede intranet usando a versão 4 do IP, ao se ligar na internet, deve trocar todos os endereços IP das máquinas conectadas a ela, com esse esquema ela pode usar seu endereço de rede e interface em conjunto com um prefixo global alocado a ela, por exemplo, com o prefixo Provider-Based.

Notação de Endereços IPv6

Com os endereços IPv6 ocupando um espaço de 16 bytes, é necessário uma nova forma de se notar os números Ip. Eles agora são escritos em 8 grupos de 4 dígitos hexadecimais cada, separados por dois pontos (:), como estes:

8000:0000:0000:0000:0123:4567:89AB:CDEF

47CD:1234:4422:AC02:0022:1234:A456:0124

Como os endereços IPv6 possuem muitos bytes em 0, três passos de otimização podem ser tomados:

1. Zeros podem ser omitidos no início do grupo. Assim, 0123 pode ser escrito como 123.
2. Um ou mais grupos com 4 bytes em 0 podem ser omitidos, substituídos por um par de dois pontos. Desta forma, o primeiro número do exemplo acima poderia ser escrito da seguinte forma: 8000::123:567:89AB:CDEF
3. Endereços IPv4 podem ser escritos por um par de dois pontos seguido da notação da versão 4. Por exemplo: ::143.54.1.20

1.5.5 Datagrama IPv6

Formato do Pacote

IPv6 muda completamente o formato do datagrama IP. Como a Figura 3.1.6 mostra, um datagrama IPv6 tem um cabeçalho base fixo seguido de 0 ou mais cabeçalhos extras, seguidos pelos dados.

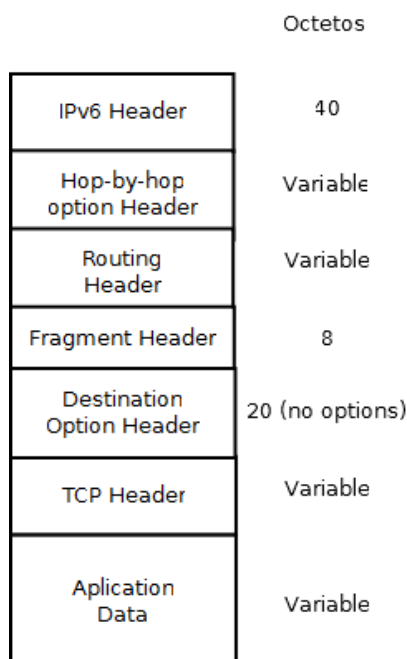



Figura 3.1.6: Formato Pacote IPv6.

Embora o IPv6 estenda o IPv4, seu cabeçalho é relativamente simples, contendo menos informações que o cabeçalho do datagrama IP da versão 4. Alguns campos do cabeçalho da versão 4 e opções foram substituídos por cabeçalhos de extensão.

Algumas mudanças no cabeçalho são:

- O campo de tamanho de cabeçalho foi eliminado, pois tem tamanho fixo de 40 bytes, substituído por um campo que indica o tamanho do que se segue ao cabeçalho.
- O tamanho dos campos de endereço passaram para 16 bytes.
- Informação de fragmentação passaram a estar em cabeçalhos de extensão.
- O campo Tempo de vida (Time-to-live) mudou para Limite de saltos (hop limit).
- O campo Tipo de serviço (Service Type) mudou para Identificação do fluxo (Flow Label)
- O campo que indicava o protocolo sendo “transportado” passou a ser um campo que indica o próximo cabeçalho.

A Figura 3.1.7 esquematiza o cabeçalho do IPv6.

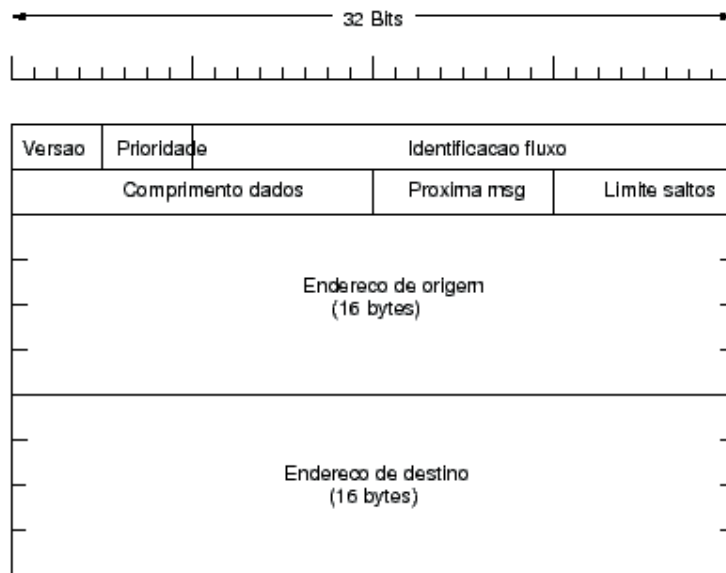



Figura 3.1.7: Cabeçalho IPv6.

Campos do cabeçalho IPv6:

Versão:

Versão do protocolo - 4 bits;

Prioridade:

Valor da Prioridade- 4 bits;

Identificação do fluxo:

Qualidade de Serviço - 24 bits;

Comprimento do dado:

Tamanho do payload, isto é, o resto do pacote que segue ao IPv6 header, excluindo este, que tem tamanho fixo de 40 octetos. Desta forma o datagrama IPv6 pode ter até 64 k - 16 bits;

Próxima msg:

Identifica o próximo cabeçalho, isto é, o protocolo acima do IP. Usa os mesmo valores da versão 4, mas vem em substituição ao campo Protocol da versão 4 - 8 bits;

Limite de saltos:

Número máximo de hops pelos quais o pacote pode trafegar. Decrementado em 1 a cada novo hop. Quando seu valor é igual a 0 o pacote é descartado - 8 bits;

Endereço de origem:

Identifica o endereço origem do pacote - 128 bits;

Endereço de destino:

Identifica o endereço destino do pacote (nem sempre o destino final, no caso de um cabeçalho opcional de roteamento estar presente - 128 bits;

Qualidade de Serviço

Os campos de Flow Label e Priority no cabeçalho são usados para identificar aqueles pacotes que necessitam de "cuidados especiais". São pacotes originados de aplicações multimídia ou de tempo real, por exemplo.

Identificação de fluxo

São 24 bits que podem ser usados para identificar um tipo de fluxo de dados (algo como uma conexão ou circuito virtual). Classifica-se em fluxo orientado aquele que demanda muitos pacotes, e fluxo não-orientado aquele que não demanda muitos pacotes, muito tráfego. A tabela 3.1.7 mostra alguns exemplos de aplicações para esses tipos de fluxos.

Tabela 3.1.7

Classificação de Tráfego conforme Aplicação	
Tráfego orientado	**Tráfego não-orientado**
FTP	DNS
Telnet	SMTP
HTTP	NTP
POP	SNMP

O uso deste campo não é explicitamente definido, mas imagina-se que um fluxo orientado necessita uma atenção maior que um fluxo não orientado. Caberia aos roteadores negociarem quais são as medidas a serem tomadas.

Prioridade

Este campo determina a prioridade do datagrama em relação a outros datagramas da mesma origem. Todos os pacotes de determinado fluxo devem ter a mesma prioridade, portanto estes são dois campos usados em conjunto. Espera-se que esse campo identifique e priorize aplicações iterativas, como sessão remota.

O uso efetivo se dá quando o pacote enfrenta um tráfego congestionado. Valores de 0 a 7 nesse campo lidam com transmissões (geralmente TCP) que podem ser retardadas no caso de um congestionamento. Valores de 8 a 15 se referem a aplicações cujo tráfego é constante e um atraso implicaria em perda de informação, como vídeo e áudio.

1.5.6 Cabeçalhos de Extensão

Ter um cabeçalho básico fixo e outros extras vem atender à necessidade de se ter generalidade e eficiência na nova versão. Para ser geral, mecanismos de fragmentação, autenticação, etc, devem ser suportados, mas devem ser incluídos somente quando necessários. Para tanto, são incluídos em cabeçalhos extras, pois se estivessem sempre presente, o cabeçalho principal do protocolo seria tão grande que o tempo de se processá-lo levaria à ineficiência da rede.

Cada cabeçalho de extensão deve ter o campo Next Header a fim de indicar o próximo cabeçalho que se segue, num processo semelhante a uma lista encadeada de dados. Na Tabela 3.1.8 mostramos 3 datagramas, o primeiro com nenhum cabeçalho extra, o segundo com 1 e o último com 2.

Tabela 3.1.8

FORMATO DO CABEÇALHO IPV6 COM EXTENSÕES			
Primeiro	**Segundo**	**Terceiro**	**Quarto**
Base Header/Next=TCP	TCP PDU		
Base Header/Next=Route	Route Header/Next=TCP	TCP PDU	
Base Header/Next=Route	Route Header/Next=Auth	Auth Header/Next=TCP	TCP PDU

Os cabeçalhos de extensão do IPv6 podem ser visto na Figura 3.1.8. A seguir apresentamos o detalhamento de cada extensão de cabeçalho.

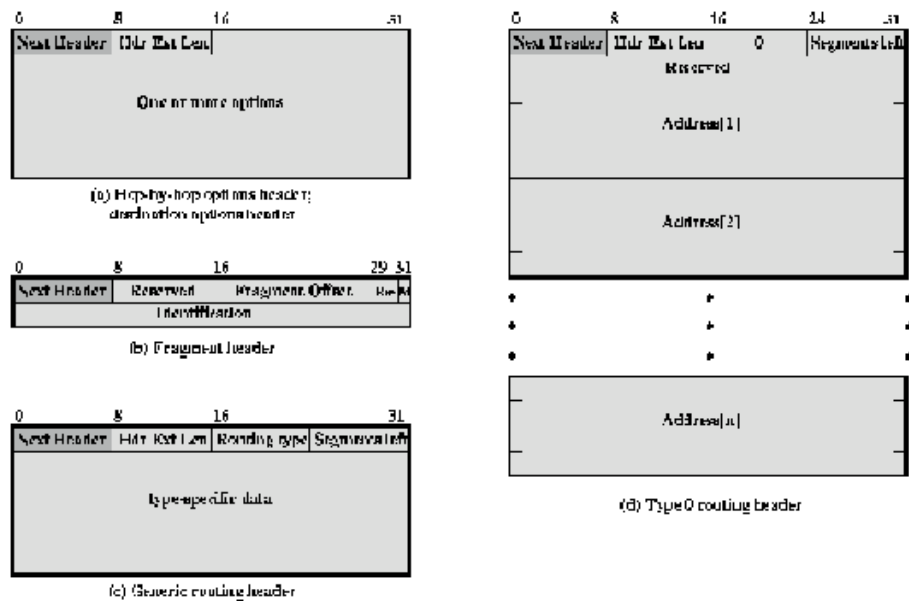



Figura 3.1.8: Cabeçalho IPv6 com Extensões.

Cabeçalhos Hop-by-Hop e Destination

Os cabeçalhos de Hop-by-hop Options e Destination Options têm o mesmo formato e são mostrados na Figura 9.8a. Eles foram projetados em

vista de reunir várias informações isoladas e simples que por si só não necessitavam de mais um cabeçalho de extensão. A parte do cabeçalho que segue ao seu tamanho é dividida da seguinte forma:

Tabela 3.1.9

Cabeçalho Hop-by-hop		
8 bits	8 bits	n bits
Type	Lenght	Value

Type indica o tipo de opção. Caso essa opção contenha dados, o tamanho dos dados é indicado em lenght. Os dados ficam presente, então, no campo value. Os 5 bits de mais baixa ordem em type indicam a opção, enquanto o terceiro bit de mais alta ordem indica se os dados dessa opção podem mudar durante o trajeto do pacote. Caso essa opção não seja conhecida por algum nó durante o caminho do pacote, os dois bits de mais alta ordem indicam a ação a ser tomada:

00

Ignore esta opção, continue o processamento de cabeçalhos

01

Descarte datagrama, mas não envie mensagem ICMP

10

Descarte datagrama e envie mensagem ICMP para a origem

11

Descarte datagrama e envie mensagem ICMP para a origem somente se o destino não for um endereço multicast

Cabeçalho de Fragmentação

Tendo em vista que no IPv4 roteadores deveriam fragmentar e reorganizar datagramas que fossem maior que que a MTU da sua rede, no IPv6 a fragmentação é toda feita na origem. Para tanto, a origem realiza um Path MTU discovery, ou uma descoberta de MTU mínimo, a fim de identificá-lo. Assim, basta fragmentar o datagrama de tal modo que ele passe por todos as redes no caminho até seu destino.

Cada fragmento deve ser múltiplo de 8 octetos, e cada cabeçalho de fragmentação indica se existem outros fragmentos do mesmo dado ou não. A Figura 9.8b mostra o cabeçalho de fragmentação.

Next Header (8 bits):

indica o próximo cabeçalho;

Reserved (8 bits):

reservado para o futuro;

Fragment Offset (13 bits):

indica aonde no pacote original este fragmento deve ser inserido, qual o seu lugar;

Res (2 bits):

reservado para o futuro;

M Flag (1 bit):

indica se existem mais fragmentos (1) ou se este é o último (0);

Identification (32 bits):

identificação do pacote original; deve ser única em toda a internet enquanto o pacote estiver trafegando.

Um problema gerado por esse tipo de fragmentação end-to-end, onde nós intermediários não podem fragmentar, é que se a rota mudar no meio da transmissão e o novo MTU for menor que aquele já descoberto, alguma coisa precisaria ser feita. O que acontece é que o datagrama IPv6 não é mexido, mas um datagrama novo é montado com o outro sendo encarado como dado. Assim, ele pode ser fragmentado no meio do caminho e remontado no meio do caminho. O que espera-se é que isso não seja muito necessário.

Cabeçalho Genérico de Roteamento

O cabeçalho de roteamento contém uma lista de um ou mais nós que devem ser "visitados" no caminho para o destino. Os cabeçalhos de roteamento, mostrado na Figura 9.8c sempre começam com um bloco de 32 bits divididos em 4 campos de 8 bits cada.

Next Header (8 bits):

identifica o próximo cabeçalho;

Header extension length (8 bits):

tamanho do cabeçalho em unidades de 64 bits, não incluindo o próprio cabeçalho;

Routing type (8 bits):

identifica um tipo de roteamento; se ele não for compreensível por algum nó no caminho, o pacote deve ser descartado;

Segments left: (8 bits):

número de nós intermediários (listados explicitamente) que devem ainda ser visitados antes do destino.

Cabeçalho de Roteamento tipo 0

Além dos 32 bits do cabeçalho de roteamento, esse tipo 0 de cabeçalho de roteamento foi definido com mais 8 bits reservados e 24 bits de strict/

loose bit map. Esses bits são numerados da esquerda para a direita, cada um correspondendo a um hop, indicando se o próximo destino deve ser um vizinho deste (1 = strict) ou não (0 = loose). O Cabeçalho de Roteamento tipo 0 é mostrado na Figura 9.8c

Quando se usa o roteamento de tipo 0, a origem não precisa informar separadamente o destino do datagrama, pois ele é considerado como sendo o último endereço listado no cabeçalho de roteamento (address [n] na Figura 9.8), sendo que o cabeçalho básico do IPv6 tem como destino o primeiro endereço listado no cabeçalho de roteamento. Antes desse nó ser atingido, o cabeçalho de roteamento não é examinado, mas quando for a hora, o próximo nó listado no cabeçalho de roteamento é colocado no cabeçalho básico, o datagrama é enviado, e o segments left é decrementado.

1.5.7 Segurança

O atual IPv4 apresenta uma série de problemas de segurança, não garantindo autenticidade e privacidade abaixo do nível de aplicação. Para a nova versão, foram projetadas duas opções que podem ser usadas separadamente ou em conjunto, de acordo com as necessidades de segurança das diversas redes.

A infraestrutura proporcionada pelo IPv6 vai requerer mais estratégias de segurança do que apontadas pelo IPv4. Mecanismos de autoconfiguração, ausentes até agora, terão de ser bem autenticadas. Opções de qualidade de serviço não muito rígidas podem tornar seus datagramas passíveis de ataque. Cuidados devem ser tomados para que uma combinação de opções não deixem os datagramas desprotegidos.

Uma palavra-chave em termos de segurança é a associação. Uma associação é um relacionamento unidirecional entre um transmissor e um receptor. Se os dois nós de uma conexão vão transmitir, então duas associações são necessárias. Cada associação é identificada por um endereço destino e um SPI - security parameter index, presente nos cabeçalhos de segurança.

Os parâmetros que definem uma associação de segurança são geralmente os algoritmos de autenticação e/ou criptografia e sua(s) chave(s).

Autenticação

A autenticação é provida por um cabeçalho de extensão que suporta a integridade e autenticação dos dados de um pacote IP.

Next header (8 bits):

identifica o próximo cabeçalho

Length (8 bits):

tamanho do campo de de dados em palavras de 32 bits

Reserved (16 bits):

reservado para uso futuro

Security parameters index (32 bits):

identifica uma associação de segurança

Authentication data (variável):

dados, em palavras de 32 bits

O que o campo de dados representará vai depender do algoritmo de autenticação usado. Mas no geral este campo é calculado com base em todo o datagrama, excluindo-se campos que mudem durante sua rota. No cálculo, esses campos são encarados como sequências de bits 0. Cabeçalhos de fragmentação podem ser incluídos no cálculo

1.5.8 Transição IPv4 / IPv6

A palavra chave na transição entre as duas versões do protocolo IP é interoperação. As duas versões devem poder permanecer na rede simultaneamente, se comunicando e endereçando. A segunda palavra chave é facilidade. Deve ser fácil se poder dar um upgrade nos softwares da versão 4 para a 6, tanto para administradores de rede, técnicos, como para o usuário final.

Os objetivos da transição são:

- roteadores e máquinas devem ter seus programas de rede trocados sem que todos os outros no mundo tenham que trocar ao mesmo tempo.
- O único pré-requisito é que os servidores de DNS devem ter a sua versão trocada antes. Para os roteadores não existem pré-requisitos
- quando as máquinas sofrerem o upgrade devem poder manter seus endereços IPv4, sem a necessidade de muitos planos de um re-endereçamento, usando inicialmente um dos prefixos vistos anteriormente
- custos baixos
- nós IPv6 devem poder se comunicar com outros nós IPv6, mesmo que a infraestrutura entre eles seja IPv4.

Para o último objetivo, dois mecanismos foram trabalhados:

- dual-stack: com esse mecanismo, nós IPv6 devem ter as duas pilhas TCP/IP internamente, a pilha da versão 6 e a da versão 4. Através da versão do protocolo, se decide qual pilha processará o datagrama. Esse mecanismo permite que nós já atualizados com IPv6 se comuniquem com nós IPv4, e realizem roteamento de pacotes de nós que usem somente IPv4

- tunneling: esse mecanismo consiste em transmitir um datagrama IPv6 como parte de dados de um datagrama IPv4, a fim de que dois nós IPv6 possam se comunicar através de uma rede que só suporte IPv4. A rede IPv4 é vista como um túnel, e o endereço IPv4 do nó final deste túnel consta como destino do datagrama. Neste nó o pacote IPv6 volta a trafegar normalmente a seu destino. Esse nó final, portanto, deve ter a pilha que suporte IPv6.

Atividades de avaliação

1. Comente a importância do protocolo IP para a infraestrutura da Internet.
2. Qual a diferença da regra de alocação de numeração entre o endereçamento IP e numeração do sistema telefônico?
3. Uma empresa tem uma rede IP constituída de 200 hosts separadas em 5 subredes, sendo 2 delas na cidade matriz e as outras 3 em filiais situadas em cidades diferentes. Considerando que são usados apenas roteadores de duas portas, qual a quantidade mínima de roteadores necessária para interligar toda a empresa? Faça um desenho da rede.
4. Qual é a maior vantagem do código de verificação de erro do datagrama IP somente cobrir o cabeçalho em vez de cobrir toda a mensagem?
5. Por que o código de verificação de erro do datagrama IP utiliza o simples Checksum em vez de CRC, que é muito mais preciso e confiável?
6. Qual é a vantagem de realizar a remontagem da mensagem somente no destino em vez de fazê-lo logo após cada trecho onde houve fragmentação?
7. Qual a função do protocolo ICMP e de exemplo de uma aplicação que o utiliza?
8. Diga o objetivo do protocolo ARP e explique seu funcionamento.
9. Existe alguma situação especial onde hosts conectados a uma rede Ethernet não precisaria de usar o protocolo ARP para transmitir um datagrama IP?
10. Quais as principais melhorias implementadas no protocolo IPv6 sobre a versão atual IPv4?
11. Como é a notação de endereços IPv6? Dê um exemplo.
12. Qual a função do campo do cabeçalho FlowLabel? Qual o campo do cabeçalho IPv4 ele substitui?
13. Qual a função do campo do cabeçalho Hop Limit? Qual o campo do cabeçalho IPv4 ele substitui?

14. Por que o cabeçalho IPv6 não tem campo de verificação de erros? O cabeçalho do IPv6 é muito maior que o cabeçalho IPv4. Como é possível que o IPv6 seja mais eficiente (processamento mais rápido) que o o IPv4?
15. Comente as medidas para tornar suave a migração do IPv4 para IPv6.
16. Uma empresa dispõe da classe C 200.100.50.0 para seu uso. Aa localidades que esta empresa tem escritório com o respectivo número de hosts e roteadores é listado na tabela abaixo. Divida os endereços IP e indique os endereços para hosts e roteadores e a máscara de cada subrede.

Local	Quant. Hosts	Quant. Roteadores
RJ	110	3
SP	55	1
BH	29	1
POA	11	1

2. Roteamento

A Internet é uma conjunto de redes interconectadas, e os pontos de ligação dessas redes são os roteadores. As redes são organizadas de forma hierárquica e agrupadas sob a mesma autoridade administrativa. Alguns roteadores são utilizados para trocar dados entre redes controlados pela mesma autoridade administrativa, enquanto outros fazem também a comunicação entre redes de diferentes autoridades administrativas. Esse agrupamento de redes controladas por uma mesma autoridade administrativa é chamado de Sistema Autônomo. Podemos dizer que a Internet é constituída por sistemas autônomos interconectados. A função de encaminhar os pacotes IP para seus respectivos destinos (redes) é chamado roteamento e são executados pelos equipamentos roteadores.

2.1 Roteamento Estático

A função de roteamento utiliza tabelas de roteamento que contém endereços de possíveis destinos e a maneira de alcançá-los. A Internet é uma rede de comutação por pacotes com roteamento descentralizado. O roteamento estático consiste em criar tabelas de roteamento fixas (estáticas) em cada roteador pertencente a rede. Em uma rede pequena e com poucas mudanças o roteamento estático é eficiente pela sua simplicidade e segurança, entretanto, com redes maiores e com mudanças frequentes a administração pode se tornar difícil. Apresentamos na Figura 10.1 um exemplo de rede com roteamento estático.

2.1.1 Tabela de roteamento

O roteamento estático consiste na definição de tabelas de roteamento para

cada dispositivo da rede. Essa definição é manual e exige um planejamento rigoroso para não haver erros.

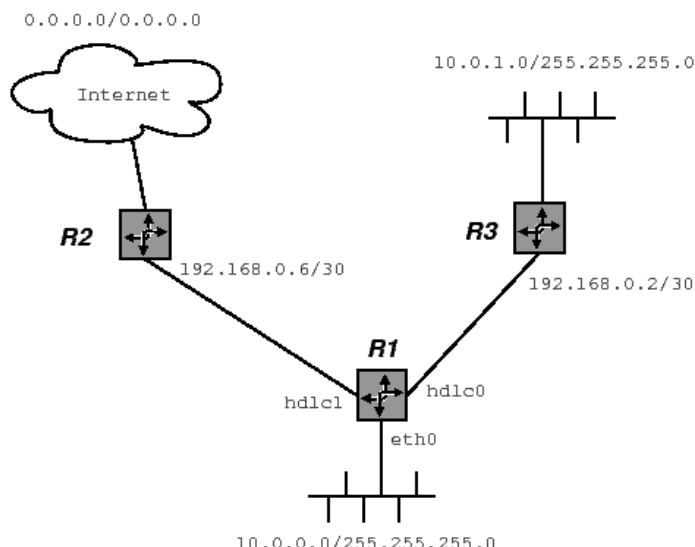



Figura 3.2.1: Exemplo de rede com roteamento estático.

Uma tabela de roteamento estático contém basicamente quatro campos:

Destino:

Endereço de destino

Gateway:

Endereço para onde se deve enviar o pacote para determinado Destino

Máscara:

Máscara da rede de destino

Interface:

Interface física por onde o pacote deve ser enviado.

Destination	Gateway	Netmask	Interface
10.0.0.0		255.255.255.0	eth0
192.168.0.0		255.255.255.252	hdlc0
192.168.0.4		255.255.255.252	hdlc1
127.0.0.0		255.0.0.0	lo
10.0.1.0	192.168.0.2	255.255.255.0	hdlc0
0.0.0.0	192.168.0.6	0.0.0.0	hdl

A primeira linha mostra o endereço da porta ethernet do roteador, e por estar diretamente conectada, não há endereço de gateway. Assim qualquer pacote para o endereço 10.0.0.0 com máscara 255.255.255.0 deve ser simplesmente

transmitido pela interface eth0, onde está o destino desejado. A segunda e terceira linha indicam o endereço das interfaces hdlc0 e hdlc1, respectivamente.

A quarta linha indica o endereço de uma interface local. Muitas aplicações TCP/IP exigem a presença de um endereço IP para funcionar adequadamente. Se fosse obrigatório uma interface para configuração de um endereço IP, um computador desconectado não poderia executar essas aplicações. Assim, a interface local é uma interface virtual com um endereço IP que é configurado automaticamente durante a fase de boot. A interface local também é importante para o correto funcionamento de protocolos de roteamentos dinâmicos, como mostraremos a seguir.

A quinta linha indica que para atingir a rede 10.0.1.0 com máscara 255.255.255.0 devemos enviar o pacote para o gateway 192.168.0.2 através da interface hdlc0. Podemos notar que a informação da interface aqui é redundante pois a segunda linha indica que a rede 192.168.0.0/255.255.255.252 está diretamente conectada à interface hdlc0.

A sexta linha é também é chamada de default gateway, que significa ser a saída padrão. Se o endereço de destino não é encontrado em nenhuma rota anterior, o pacote é transmitido para esse endereço (gateway). Note que o endereço e máscara 0.0.0.0/0.0.0.0 serve para qualquer endereço IP. Mais uma vez, o nome da interface é redundante, pois o gateway pertence a rede da terceira linha.

2.2 Roteamento Dinâmico

O roteamento estático é confiável e seguro, e foi largamente utilizado no início da Internet. Porém com o crescimento da rede a administração tornou-se difícil exigindo a criação de mecanismos de roteamento dinâmico, onde a alteração de uma rota não exigisse a modificação de todas as rotas individualmente em cada equipamento da rede.

2.2.1 Algoritmos de Roteamento Dinâmico

A propagação automática de rotas permite a divulgação de rotas para o funcionamento coerente de uma rede com um mínimo de interferência de operador humano. Os algoritmos de propagação de rotas mais conhecidos são:

- Vetor Distância (Vector Distance)
- Estado de Enlace (Link State)

Roteamento Vetor Distância (Vector Distance)

Esse algoritmo também é conhecido como Bellman-Ford. É o mecanismos mais simples, baseado na distância entre dois pontos. Essa distância refere-se ao número de roteadores existentes na rota utilizada, sendo medida em saltos (Hops). No início, a tabela de roteamento de um roteador apresenta apenas os

endereços das redes diretamente conectadas com distância zero. Periodicamente os roteadores enviam cópias das suas tabelas de roteamento para todos os roteadores vizinhos que avaliam essas rotas e atualizam suas tabelas.

A grande vantagem desse algoritmo é a simplicidade e a maior desvantagem é que não deve ser utilizado em redes grandes. Com o crescimento do número de redes, cresce também o tamanho das tabelas de roteamento, aumentando o tráfego para a manutenção das tabelas, pois é necessário transmitir toda a tabela de roteamento a cada atualização.

Roteamento Estado de Enlace (Link State)

Esse algoritmo, também conhecido como Shortest Path First (SPF), mantém um mapa da topologia da rede em cada roteador ao invés de uma tabela de roteamento. A tarefa de cada roteador é testar a possibilidade de comunicação com todos os roteadores adjacentes. De posse do estado do enlace (ativo ou não), o roteador divulga as informações para os outros roteadores.

A escolha da melhor rota é efetuado em cada roteador através do algoritmo "Dijkstra Shortest Path", que calcula o caminho mais curto para o destino desejado a partir dele, utilizando sempre a menor distância com enlaces ativos. A grande vantagem dos algoritmos SPF reside no fato das mensagens enviadas serem pequenas, o que diminui o tráfego para difundir informações de roteamento.

2.2.2 Protocolos de Roteamento Dinâmico

Os protocolos de roteamento utilizam um dos algoritmos acima e podem ser aplicados em redes IGP (Interior Gateway Protocol) ou EGP (Exterior Gateway Protocol). Os protocolos IGP são utilizados dentro de um mesmo sistema autônomo (AS) enquanto os protocolos EGP são utilizados entre sistemas autônomos diferentes.

A Internet é constituída por sistemas autônomos interconectados e a definição de uma rede com sistema autônomo é que ela mantêm todas as rotas da Internet e pode transmitir um pacote mesmo que uma ligação esteja interrompida. Qualquer rede ligada à mais de um provedor de comunicações, necessariamente é um sistema autônomo.

Apresentamos na tabela 3.2.1 as características dos protocolos de roteamento dinâmico mais utilizados:

Tabela 3.2.1

Protocolos de Roteamento Dinâmico		
Protocolo	**Algoritmo**	**Localização**
RIP	Vetor Distância	IGP
OSPF	Estado de Enlace	IGP
BGP-4	Vetor Distância	EGP

2.3 RIP (Routing Information Protocol)

O protocolo RIP é um protocolo de roteamento dinâmico que implementa o algoritmo vetor-distância. Em seu método os equipamentos são classificados em ativos e passivos(silenciosos). Roteadores ativos informam suas rotas para outros e os passivos apenas escutam e atualizam suas rotas baseadas nas informações recebidas, mas não informam. Tipicamente, os roteadores usam RIP em modo ativo, enquanto as estações (hosts) usam em modo passivo.

Um roteador com RIP no modo ativo envia para a rede uma mensagem com as informações de suas rotas a cada 30 segundos. Cada mensagem consiste informações de um endereço IP de rede de destino e uma distância da rede (número de saltos). RIP usa uma métrica de contagem de saltos para medir a distância ao destino, onde cada salto corresponde a um roteador até o destino. Nem sempre o menor número de saltos significa a melhor rota, por exemplo, uma rota mais longa com melhor qualidade de linhas pode ser melhor, porém o RIP não tem recursos para fazer essa avaliação.

Roteadores RIP, ativos ou passivos, ouvem todas as mensagens broadcast e atualizam suas tabelas de acordo com o algoritmo vetor-distância, isto é, aceita uma nova rota recebida se ela for mais curta (menos saltos) para o destino.

Existem duas versões de protocolo RIP: versão 1, definida pelo RFC 1058, e a versão 2, especificada pelo RFC 2453. A diferença é que a versão 2 aceita subredes (a versão 1 não tem máscara) e implementa um mecanismo de autenticação, para evitar que uma rede aceite rotas erradas de equipamentos estranhos à rede. A versão 1 é considerada obsoleta e, praticamente, apenas a versão 2 é utilizada. Nesse texto são considerados apenas funcionalidades da versão 2.

2.3.1 Funcionamento do Protocolo RIP

Podemos observar na Figura 3.2.2 uma topologia de rede constituída por 3 subredes, 3 roteadores e 2 estações. Neste exemplo os roteadores tem o protocolo RIP no modo ativo e as estações no modo passivo.

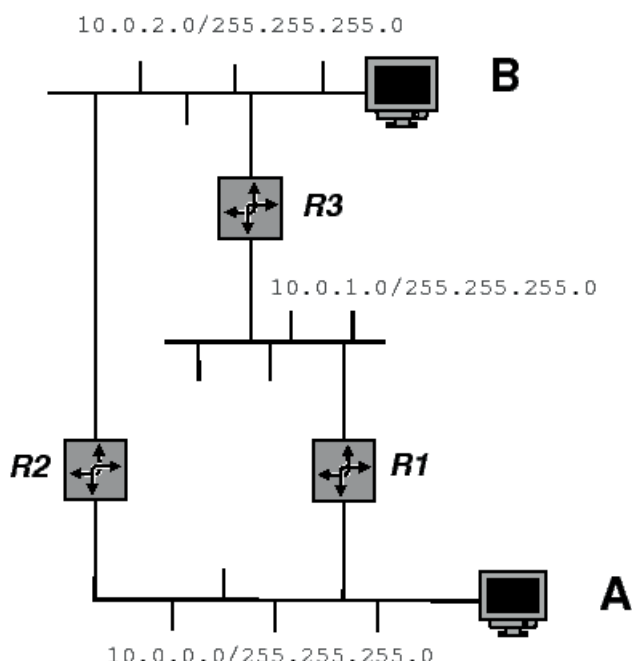



Figura 3.2.2: Exemplo do protocolo RIP.

Ao ativar o protocolo RIP as estações e os roteadores incluem em suas tabelas as rotas diretamente conectadas. A estação A fica com a seguinte tabela de rotas:

oÉÇÉ	jłëÅ~ê~	`~ãáåÜç	jÝíêáÅ~
NMKMKMKM	ORRKORRKORRKM	içÅ~ä	M

Como a estação A funciona no modo passivo, ela não divulga rotas, apenas escuta.

Ao ativar o protocolo no roteador R1, as redes diretamente conectadas são incluídas.

oÉÇÉ	jłëÅ~ê~	`~ãáåÜç	jÝíêáÅ~
NMKMKMKM	ORRKORRKORRKM	içÅ~ä	M
NMKMKNKM	ORRKORRKORRKM	içÅ~ä	M

Após incluir as redes diretamente conectadas, irá divulgar suas rotas para os vizinhos, pois funciona em modo ativo. O roteador R1 também irá receber rotas de outros roteadores, por exemplo, O roteador R3. Após receber a tabela de R3 a tabela de R1 fica:

oÉÇÉ	jłëÅ~ê~	`~ãáåÜç	jÝíêáÅ~
NMKMKMKM	ORRKORRKORRKM	içÅ~ä	M
NMKMKNKM	ORRKORRKORRKM	içÅ~ä	M
NMKMKNKM	ORRKORRKORRKM	oP	N
NMKMKOKM	ORRKORRKORRKM	oP	N

A métrica das rotas recebidas de R3 recebem o valor 1, pois para o roteador R1 é necessário passar por R3 para chegar a esses destinos. O roteador R1 recebe uma outra rota para a rede 10.0.1.0, através de R3, mas ela é descartada porque existe uma rota melhor com métrica 0, já que essa rede está diretamente conectada a ele. O roteador R1 também recebe uma rota para 10.0.2.0 através de R2, mas como ela tem a mesma métrica do caminho R3 ela é desprezada. Assim a tabela de roteamento de R1 fica:

oÉÇÉ	jłëÅ~ê~	`~ãáåÜç	jÝíêáÅ~
NMKMKMKM	ORRKORRKORRKM	içÅ~ä	M
NMKMKNKM	ORRKORRKORRKM	içÅ~ä	M
NMKMKOKM	ORRKORRKORRKM	oP	N

Como o roteador R1 funciona em modo ativo, ele divulga sua tabela de rotas para estação A, que fica com a seguinte tabela de roteamento:

oÉÇÉ	jłëÅ~ê~	`~ãáåÜç	jÝíêáÅ~
NMKMKMKM	ORRKORRKORRKM	içÅ~ä	M
NMKMKNKM	ORRKORRKORRKM	oN	N
NMKMKOKM	ORRKORRKORRKM	oN	O

No entanto, a estação A também recebe rotas do roteador R2 que tem um melhor caminho (menor métrica) para atingir a rede 10.0.2.0 através dele, então a tabela final da estação A fica:

oÉÇÉ	jłëÅ~ê~	`~ãáåÜç	jÝíêáÅ~
NMKMKMKM	ORRKORRKORRKM	içÅ~ä	M
NMKMKNKM	ORRKORRKORRKM	oN	N
NMKMKOKM	ORRKORRKORRKM	oO	N

A tabela é renovada a cada 30 segundos e caso algum canal pare de funcionar, o roteador não mais transmite essa rota. Se uma rota não é atualizada por mais de 180 segundos, ela tem sua métrica alterada para infinito (na prática 16), indicando que o caminho não é mais acessível.

Em nosso exemplo, caso R2 pare de funcionar ele deixa de enviar a rota da rede 10.0.2.0 e a estação A muda a métirca dessa rota para 16 (infinito). Se a rota por R1 e R3 estiver ativa, R2 envia uma mensagem com rota para 10.0.2.0 com métrica 2. Como 2 é menor que 16 (infinito), a estação A passa a utilizar o caminho R1 para chegar à estação B. Se o roteador R2 voltar a funcionar, a estação A receberá uma rota para 10.0.2.0 com métrica 1, que substituirá a rota via R1, e voltará a situação original.

Quando há dois roteadores que atingem uma determinada rede e essa conexão é interrompida, por causa do atraso na atualização das rotas, ambos propagam rotas que atingem essa rede através do outro roteador, mas não poderão porque ela está inacessível. Para esse tipo de problemas foram desenvolvidos alguns mecanismos para melhorar a convergência lenta.

2.3.2 Problemas do protocolo RIP

O protocolo RIP estabelece poucas regras para performance e para prevenir rotas oscilantes entre dois ou mais hosts com caminhos de mesmo custo, especifica que estas rotas devem ser guardadas até a descoberta de uma com custo mais baixo. Em caso de falha física em um gateway ou de um gateway informar que uma rota ter falha RIP especifica que todos os ouvintes devem colocar "timeout" nas rotas aprendidas, pois um quando um gateway instala uma rota em uma tabela coloca um "timer", este tempo deve ser recomeçado a cada vez que o gateway recebe outra mensagem RIP informando a respeito da rota. A rota torna-se inválida se 180 segundos passam sem que a rota tenha sido notificada novamente.

O protocolo RIP apresenta os seguintes problemas básicos: loops em roteamento, limitação de saltos, e convergência vagarosa ou contagem ao infinito. O protocolo RIP em seu algoritmo não especifica detecção de loops de roteamento. RIP assume que cada participante deve ser confiável ou tomar precauções para prevenir cada loop. Em segundo, para prevenir instabilidades RIP deve-se usar um baixo valor para representar a máxima distância alcançável em saltos entre gateways. O administrador da rede deve usar um protocolo alternativo para Internet em qual torne viável o número de saltos para roteamento entre gateways até o limite de 16. Esta limitação de saltos torna o RIP inconveniente para grandes redes.

O algoritmo vetor distância usado pelo RIP cria uma convergência vagarosa ou contagem ao infinito, problema em que as inconsistências surgem porque o roteamento atualiza as mensagens propagadas vagarosamente através da rede. A escolha de um pequeno limite (16) atenua o limite de convergência mas não a elimina.

O problema de convergência vagarosa pode ser resolvido de três maneiras:

- Split horizon
- Hold down
- Poison reverse

Split Horizon

No uso de Split Horizonte um gateway recorda a interface sobre o qual ele recebeu uma particular rota e não propaga esta informação a respeito da rota anterior sobre o mesmo interface.

Pode-se pensar o Slipt Horizonte em termos de fluxo de informações, um gateway informa um rota curta de acesso a uma rede, todas os gateways recebem e respondem, rapidamente, para instalar esta rota. Se um gateway para de informar uma rota o protocolo depende de um mecanismo de time-

-out antes de considerar a rota inalcançável. Uma vez que o time-out ocorre, o gateway acha uma rota alternativa e dispara a propagação desta informação.

Desafortunadamente, um gateway não pode saber se a rota alternativa depende da rota que esta interrompida. Esta negativa de informação não se propaga rapidamente.

Hold down

Uma outra técnica utilizada para resolver o problema da convergência vagarosa é o Hold Down. No Hold Down força-se um gateway participativo a ignorar a informação sobre uma rede por um período fixo de tempo seguindo o recebimento de uma mensagem que reclama que a rede está inalcançável.

O Hold Down período é setado em 60 segundos, a ideia é esperar um tempo longo o suficiente para assegurar que todas as máquinas receberam as más notícias e não se confundiram aceitando uma mensagem que esta fora de data. Deve-se ressaltar que todas as máquinas que estiverem usando RIP com Hold Down devem ter versões idênticas de Hold Down ou loops de roteamento podem ocorrer.

A desvantagem da técnica é que se loops de roteamento ocorrem, eles serão preservados durante o período de Hold Down, preserva-se todas as rotas incorretas sempre que a alternativa existe.

Poison Reverse

A técnica de Poison Reverse consiste em uma vez uma conexão desaparecer, o gateway informará das conexões, para conservar as entradas das conexões, com o objetivo de manter atualizada periodicamente e incluir um infinito custo nos broadcast. Para o Poison Reverse ser mais eficiente ele deve ser combinado com disparos de atualizações.

2.4 OSPF (Open Shortest Path First)

O Open Shortest Path First (OSPF) é um protocolo do tipo estado de enlace (link-state), usado dentro de um sistema autônomo (AS), que foi definido no RFC 2328. Como se trata de um protocolo estado de enlace, os roteadores trocam informações sobre os estados dos canais de comunicação em que estão ligados.

2.4.1 Componentes de uma arquitetura OSPF

Para uma melhor distribuir das tabelas de roteamento, o protocolo OSPF implementa o conceito de "Área", onde uma rede pode ser dividida em várias áreas.

Cada área é identificada por um número diferente qualquer dentro do AS, exceto a rede central (backbone) que recebe o identificador zero (área 0). A área 0 (backbone) é a rede de trânsito e todas as áreas devem fazer contato direto com ela. Se uma rede OSPF tem apenas uma área ela deve ser denominada área 0.

O backbone é conectado as demais áreas através dos roteadores de borda de área (ABR). As informações de roteamento são enviadas para os roteadores no backbone, que propagam as informações para os demais roteadores nas bordas das áreas e assim por diante. Na Figura 3.2.3, a seguir, tem-se um exemplo de uma topologia OSPF dividida em áreas e com os diversos componentes de uma rede.

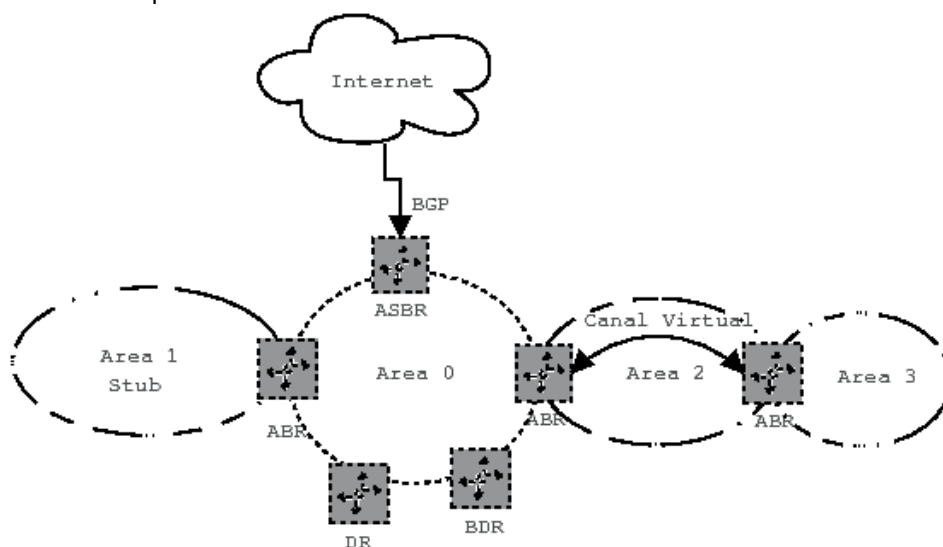



Figura 3.2.3: Componentes de uma rede OSPF.

Todas as áreas devem ter uma ligação com a área 0. Se não for possível uma ligação física, um canal virtual (link virtual) é estabelecido. Esse canal fornece um caminho lógico entre uma área e o backbone, e é estabelecido entre dois roteadores localizados nas fronteiras das áreas.

O OSPF realiza atualizações (updates) ponto a ponto. Porém, quando há na rede suporte a broadcast, por exemplo rede local, é eleito um roteador mestre (DR - Designated Router) que faz a distribuição de todas as atualizações com objetivo de agilizar a entrega das atualizações. O roteador DR é escolhido tomando como base o maior valor de prioridade ou maior identificação do roteador (RID Router ID). O valor do RID é definido na configuração do OSPF, geralmente é o um endereço IP de interface loopback do roteador ou o maior endereço IP dentre todas as suas interfaces físicas. Um segundo roteador mestre (BDR Backup Designated Router) é escolhido como alternativa em caso de falha no primeiro DR, e que é escolhido conforme segunda maior valor de prioridade ou RID da rede.

O OSPF também permite o anúncio, para um AS, de rotas descobertas de outros AS´s externos, através da redistribuição de rotas de outros protocolos para o OSPF (por exemplo, BGP). Esse roteador é chamado Autonomous System Border Router (ASBR). Um ASBR pode também conectar redes internas com RIP.

Se houver uma área localizada na borda de outra área e com apenas um roteador ABR de conexão pode constituir uma rede stub. A característica dessa rede é que o endereço do roteador ABR é único para qualquer rede que se deseje alcançar, assim o endereço do roteador ABR pode ser um default gateway e é difundido assim para toda a rede pertencente a essa área. Essa simplificação reduz muito a quantidade de mensagens difundidas e simplifica a construção da rede, melhorando o desempenho global.

2.4.2 Funcionamento do protocolo OSPF

Cada roteador OSPF armazena uma base de dados com a topologia da rede e a partir dela é construída a tabela de roteamento. O roteador que utiliza um algoritmo SPF tem duas tarefas principais:

1. Testa o estado (status) de todos os roteadores próximos periodicamente. Para realizar esse teste o roteador troca mensagens curtas (HELLO) para saber se os vizinhos estão ativos. Se o vizinho responder dentro de um certo período de tempo significa que está ativo, senão ele está inativo;
2. Publica periodicamente informações de estado dos enlaces (LSA´s - Link State Advertisements) para os demais roteadores. Para informar todos roteadores, cada roteador difunde periodicamente uma mensagem LSA que realaciona a situação de cada um de seus canais.

As mensagens do protocolo OSPF são implementados em cima do IP e são chamadas: HELLO, EXCHANGE e FLOODING. A mensagem HELLO é responsável por verificar se os canais de comunicação estão operacionais. A mensagem EXCHANGE é responsável pela sincronização inicial das bases de dados da topologia da rede. A mensagem FLOODING é responsável em manter as bases de dados da topologia da rede sincronizadas.

As mensagens geradas por um roteador podem informar: os estados e os custos dos canais de comunicação aos quais o roteador está conectado; as redes que fazem parte do AS, mas que estão fora da área; os destinos externos aos AS´s ou uma rota default para fora do AS e os roteadores ativos nessa área.

O protocolo OSPF incorpora a obrigação de uma autenticação, para evitar que rotas erradas difundida por roteadores externos causem instabilida-

de no roteamento de uma rede. Ao contrário do RIP II que oferece a autenticação como opcional, o OSPF exige a autenticação, mesmo que seja com uma senha em branco. Opcionalmente pode-se usar criptografia hash MD5 para garantir maior segurança na autenticação dos roteadores.

É requerida uma certa quantidade de memória dos roteadores para o armazenamento da tabela de roteamento e da base de dados com as informações sobre os canais, por isso apesar de ser um protocolo econômico quanto a necessidade de recursos de rede, ele requer uma quantidade não desprezível de recursos computacionais

2.5 BGP-4 (Border Gateway Protocol Version 4)

O BGP é um protocolo de roteamento dinâmico TCP/IP usado para troca de rotas entre sistemas autônomos ou Autonomous System (ASs) na Internet. O BGP é um protocolo de path vector, isto é, utiliza a filosofia vetor-distância (algoritmo Bellman-Ford), no entanto, a distância é representada pela quantidade de ASs e não quantidade de saltos, como no protocolo vetor-distância. O BGP substituiu o protocolo EGP, para sanar deficiências como: "loops" de roteamento e impossibilidade de implementação de políticas de roteamento entre ASs. A versão 4 do BGP foi a primeira versão a suportar endereços CIDR (Classless Interdomain Routing) e é atualmente a versão recomendada para uso na Internet. O protocolo BGP-4 utiliza TCP para realizar a troca de mensagens, visando a confiabilidade da comunicação.

O protocolo BGP-4 não realiza a difusão de rotas internas do AS, que deve ser realizado através de um protocolo IGP (Interior Gateway Protocol) como o RIP, OSPF ou rotas estáticas. O BGP constrói uma lista dos ASs para se chegar a uma determinada rede, usando as informações trocadas com os "vizinhos" (BGP neighbors). Esta lista é compostas pelos números identificadores dos ASs, chamada de ASN (Autonomous System Number).

Apesar de ser um algoritmo path-vector, o BGP-4 atualiza as tabelas de rotas de forma incremental, semelhante aos algoritmos de estado de enlace. A atualização completa da tabela de rotas é feita somente quando se estabelece uma sessão entre os vizinhos(neighbors).

2.5.1 Componentes de uma arquitetura BGP

Apresentamos na Figura 10.4 um exemplo de rede com os diversos componentes de uma arquitetura BGP. Roteadores que são "vizinhos " (neighbors) comunicam-se através de sessões estabelecidas entre eles. As sessões podem ser internas (iBGP) ou externas (eBGP). Os roteadores de "borda" (border routers) de ASs adjacentes são chamados peers. Esses peers fazem par-

te da fronteiras política dos ASs, que trocam tráfego de acordo com as regras definidas pelos ASs participantes.

Existem situações em que os vizinhos BGP pertencem a um mesmo AS. Quando isso ocorre existe redundância de ligação com o provedor externo, pois o tráfego pode ser dividido entre eles e a rede automaticamente desvia o tráfego para um roteador quando o outro para de funcionar. Assim, as sessões estabelecidas entre eles acontece internamente ao AS. Esta sessão é chamada iBGP (internal BGP), que permite a troca de rotas no mesmo AS. Quando a troca de rotas é realizada entre ASs diferentes chamamos de eBGP (exterior BGP). Uma característica importante do iBGP é que os neighbors não têm a obrigação de estar diretamente conectados. O eBGP trabalha, basicamente, anunciando todas rotas que conhece, enquanto o iBGP faz o possível para não anunciar rotas. Assim, é recomendado estabelecer sessões BGP entre todos os roteadores iBGP dentro de um AS, formando uma malha completa (full mesh) de sessões iBGP (AS 20 na Figura 3.2.4).

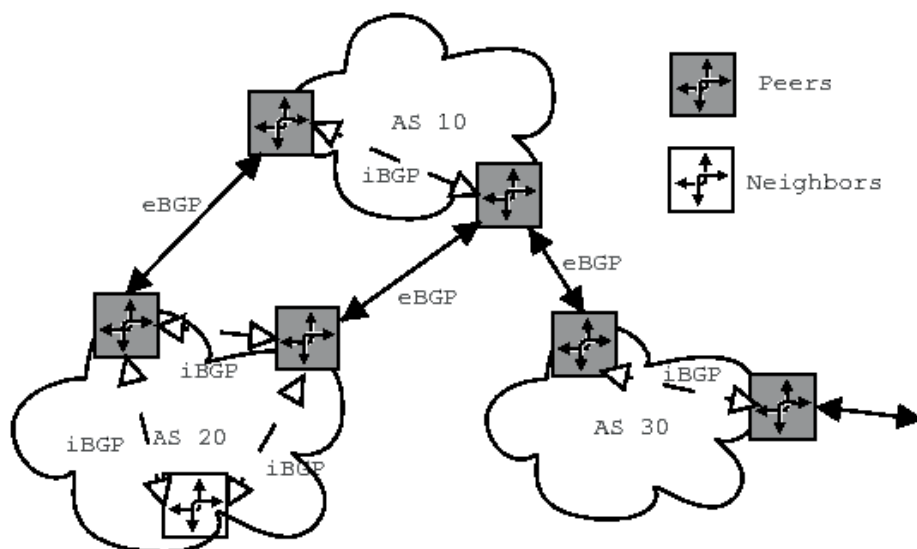



Figura 3.2.4: Componentes de uma arquitetura BGP.

2.5.2 Funcionamento do BGP

Antes do estabelecimento de uma sessão BGP, os roteadores vizinhos BGP trocam mensagens entre si para entrar em acordo sobre quais serão os parâmetros da sessão, por exemplo, tempo máximo de espera entre mensagens - hold time. Não havendo discordância ou erros durante a negociação dos parâmetros, a sessão BGP é estabelecida. Caso contrário, a sessão não será aberta.

Quando a sessão é estabelecida entre os roteadores, são trocadas mensagens com todas as informações de roteamento, ou seja, os melhores

caminhos (best path) para todos os destinos conhecidos previamente selecionados por cada peer. Após a carga inicial, eles trocarão somente mensagens de atualização das informações de roteamento (mensagens UPDATE) de forma incremental. Esse mecanismo mostrou-se eficiente para diminuir a carga nas CPUs dos roteadores e diminuir a necessidade de banda dos enlaces.

Podemos afirmar que o BGP é bastante eficiente, enviando apenas mensagens de atualizações quando ocorrem mudanças nas rotas (ex.: uma rota se tornou inválida) e informando novas rotas. Caso não ocorram atualizações, os roteadores trocam apenas mensagens de manutenção (KEEPALIVE) para verificar se a comunicação entre eles está ativa. Essas mensagens são pequenas (19 bytes), não sobrecarregando a CPU dos roteadores nem o enlace entre eles. As mensagens KEEPALIVE ocorrem apenas entre roteadores vizinhos, que são os responsáveis pela atualização das informações de roteamento.

As tabelas de rotas BGP têm um número de versão, que é incrementado a cada atualização (através das mensagens UPDATE), permitindo uma verificação de inconsistências das informações de roteamento.

No estabelecimento de uma sessão BGP entre vizinhos ocorrem os seguintes passos:

1. Estabelece uma conexão TCP entre os dois roteadores vizinhos que trocam mensagens de abertura da sessão e negociam os parâmetros de funcionamento;
2. Ambos os vizinho trocam suas tabelas de rotas BGP completa, com a relação de ASs para cada rede. Após essa etapa, as atualizações são feitas incrementalmente, conforme ocorram as mudanças de rotas;
3. Para garantir a consistência da tabela, o roteador mantém a versão da tabela que cada um dos vizinhos possuem, enquanto durar a sessão. Se a sessão for interrompida o processo é reiniciado a partir do primeiro passo;
4. Mensagens keepalive são enviadas periodicamente para manter a sessão aberta;
5. Mensagens de aviso são enviadas quando ocorrem erros;
6. Caso o vizinho identifique um erro ou receba uma mensagem de aviso, a conexão é fechada, e a sessão é encerrada.

O BGP-4 é usado quando uma rede precisa se conectar a mais de um provedor (backbone) simultaneamente, que é chamada de rede multi-homed. O roteador BGP-4 dessa rede recebe a tabela de rotas dos roteadores vizinhos do provedor e estabelece a melhor saída para atingir uma determinada rede. Além disso ele anuncia para os seus vizinhos sua

própria rede para os demais ASs, de forma que qualquer roteador da Internet possa achá-lo.

Em um roteador, cada protocolo de roteamento mantém a sua própia tabela de rotas, enquanto o roteador mantém sua própria tabela, associada ao núcleo do sistema operacional, que realmente realizam o encaminhamento de pacotes. Obviamente, os protocolos de roteamento interagem com o sistema operacional para atualizar suas tabelas, e a redistribuição ocorre quando um protocolo de roteamento repassa as rotas de sua tabela para outro protocolo de roteamento.

A redistribuição é importante para o protocolo BGP-4 pois ele não divulga rotas internas, que deverão ser feitas pelos protocolos RIP, OSPF ou rotas estáticas. Isso pode ser perigoso, pois podemos difundir todas as rotas internas do AS no BGP desnecessariamente. Todas rotas aprendidas pelo BGP não precisam ser propagadas internamente, geralmente basta apenas a rota padrão (default route). Uma filtragem cuidadosa pode ser realizada para evitar esses problemas.

2.5.3 Parâmetros do BGP

O protocolo BGP determina um conjunto de parâmetros para controlar informações relativas ao tratamento das rotas, como por exemplo, informação sobre o caminho (path), preferência da rota e o valor do próximo salto da rota. Esses parâmetros são usados pelo algoritmo BGP como elementos para decisão da escolha das rotas.

Caminho de ASs (AS_Path)

AS_Path é a sequência de ASNs que uma rota deve usar para alcançar uma determinada rede de destino. O AS que origina uma rota inclui seu ASN na lista anunciada para seus vizinhos BGP externos. Assim, cada AS que receber a lista de rotas, acrescenta seu próprio ASN no início da lista e a repassa para os outros vizinhos seus, que farão o mesmo. A lista final vai representar todos os ASNs de uma rota para chegar à rede do AS original.

Quando um AS recebe uma mensagem de rotas que contenha seu próprio ASN na seqüencia do AS_Path, esta mensagem será descartada, garantindo portanto, que não haverá loop de roteamento. Se o AS_Path é anunciado para um vizinho do mesmo AS, a informação contida no AS_Path não é alterada. A informação do AS_Path é usada no processo de seleção da melhor rota para determinado destino. Ao comparar duas rotas para um mesmo destino, o BGP vai preferir a que possuir o AS_Path menor, isto é, o caminho mais curto.

Próximo Salto (Next_Hop)

Esse atributo define o endereço IP do próximo salto, isto é, para onde o pacote deve ser enviado. Basicamente, este atributo recebe o endereço IP da interface do próximo roteador para se chegar a determinado destino.

O comportamento desse atributo é diferente para iBGP e eBGP. Em sessões eBGP, o atributo Next_Hop será sempre o IP do roteador de borda do AS vizinho que originou a rota. Em sessões iBGP o Next_Hop será o endereço IP do vizinho que anunciou a rota inicialmente. O Next_Hop aprendido pelo eBGP não é alterado pelo iBGP. Quando a rota é anunciada em rede multiacesso (Ethernet), o Next_Hop é o endereço IP da interface do roteador conectadao à rede que originou a rota.

Métrica (MED - Multi_Exit_Discriminator)

O atributo MED tem como finalidade informar aos vizinhos BGP externos (peers) o melhor caminho para uma determinada rede do próprio AS, isto é, indica aos vizinhos qual caminho deve ser seguido quando o AS possuir vários pontos de entrada.

O MED é anunciado somente entre ASs adjacentes. Só o AS de origem pode anunciar valores desse atributo, enquanto o AS vizinho que o recebe via mensagem UPDATE, que não pode repassar a outros ASs. Esse atributo só tem validade quando dois ASs são conectados com várias ligações. Se a métrica for anunciada para vizinhos BGP diferentes não há influência na mudança dos caminhos.

Preferência Local (Local Preference)

O atributo preferência local serve para anunciar o caminho preferencial de saída de pacotes para uma determinada rota externa ao AS. Esse atributo é anunciado apenas para roteadores vizinhos dentro de um mesmo AS (iBGP), não tendo influência nos roteadores vizinhos externos (eBGP).

Comunidade (Community)

O atributo comunidade é usado para representar um agrupamento de destinos com características semelhantes. Uma comunidade (community) podem ser compostas por diversas redes pertencentes a diversos ASs, e tem a finalidade de simplificar políticas de roteamento identificando rotas por um parâmetro lógico ao invés de prefixos CIDR ou ASNs. Com esse atributo, um roteador pode determinar com mais facilidade quais rotas devem ser aceitas, descartadas, preferidas ou repassadas para outros vizinhos.

Peso (Weight)

Esse parâmetro influencia no processo de seleção da melhor saída que o roteador deve usar. Por ser um atributo local, não é propagado aos seus vizinhos. Se houver mais de uma possível rota para um mesmo destino, o BGP-4 seleciona aquela que possuir o Peso (Weight) com maior valor. Este atributo é comumente usado pelos operadores de redes para equilibrar o tráfego de saída de um As.

Sincronização (Sincronization)

Esse parâmetro permite que um AS divulgue rotas de outros ASs para um

determinado vizinho (peer), possibilitando que ele se transforme em roteador de trânsito entre outros ASs. O normal de um um roteador de borda é que ele permita o tráfego entre ASs, no entanto, em algumas situações isso não é desejado, por exemplo, um ISP se ligando a dois provedores de infraestrutura (backbone).

Atividades de avaliação

1. Explique como funciona o roteamento estático em uma rede IP. Dê um exemplo de tabela de roteamento.
2. Abaixo mostramos um exemplo de tabela de roteamento. Explique o significado de cada linha:

Destino	Gateway	Máscara	Métrica	Iface
10.0.0.2	0.0.0.0	255.255.255.255	0	eth0
10.0.0.0	0.0.0.0	255.0.0.0	0	eth0
127.0.0.0	0.0.0.0	255.0.0.0	0	lo
0.0.0.0	10.0.0.2	0.0.0.0	0	eth0

3. Uma rede é constituída por 5 subredes, sendo que a rede 1 é central. A conexão utiliza protocolo PPP, por isso cada ligação deve ter endereço IP. Na rede 1 existe um roteador com 4 linhas, cada uma para cada uma das outras localidade. Distribua as classes C 10.10.1.0, 10.10.2.0, 10.10.3.0, 10.10.4.0 e 10.10.5.0 para cada localidade. Nas ligações PPP utilize a classe C 10.0.0.0. Desenhe esta rede, distribua os endereços IP e estabeleça as rotas estáticas de cada roteador (use default gateway se possível). (Atenção: cuidado com as subredes das ligações PPP)
4. Qual a vantagem e desvantagens de se utilizar o roteamento dinâmico no lugar de roteamento estático?
5. Relacione os tipos de algoritmos de roteamento dinâmico e diga as características de cada um.
6. Qual o algoritmo de roteamento dinâmico utilizado pelo protocolo RIP? Explique seu mecanismo de funcionamento.
7. Quais os principais problemas do protocolo RIP? Relacione as técnicas que resolvem estes problemas.

3. Transporte

A primeira camada que trata da comunicação fim-a-fim é a de Transporte. Ela realiza funções semelhantes à camada de enlace como controle de fluxo e controle de erros, mas no âmbito da comunicação fim-a-fim. A outra função importante é a multiplexação das diversas aplicações (camadas superiores)

em uma mesma interface de comunicação. A seção 11.1 apresenta as funções da camada de transporte, a seção 11.2 mostra o protocolo UDP e, finalmente, a seção 11.3 apresenta o protocolo TCP.

3.1 Funções da camada de Transporte

A ISO estabeleceu que há a necessidade de controlar o transporte de dados do sistema fonte para o destino para que o serviço de comunicação seja eficaz. Com isso criou-se a camada de transporte em cima da camada de rede para aliviar entidades de camadas superiores das tarefas do transporte de dados entre elas. O diagrama da camada de Transporte é mostrada na Figura 3.3.1.

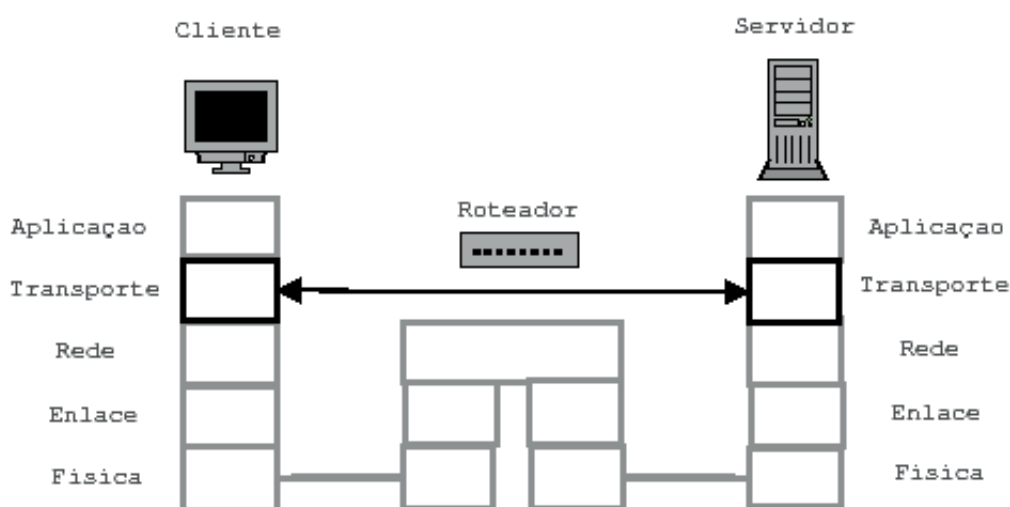



Figura 3.3.1: Diagrama da camada de Transporte.

O propósito da camada de transporte é fornecer serviço de transferência transparente de dados entre entidades da camada de sessão. O termo “transparente” refere-se ao fato de que as entidades superiores (usuários de transporte) não tem a necessidade de conhecer os detalhes pelos quais é alcançada uma transferência de dados confiável e econômica.

A função mais importante do protocolo de transporte é realizar a multiplexação dos diversos fluxos das aplicações em uma mesma entidade de transporte. Cada usuário de transporte é identificado pelo seu endereço de transporte, tanto para o lado do cliente como do lado servidor.

Os protocolos de transporte são divididos em dois grupos: orientados à conexão ou não orientados à conexão. O protocolo não orientado à conexão oferece apenas a função de multiplexação além dos serviços oferecidos pela camada de Rede. O protocolo orientado à conexão implementa o mecanismo de controle de conexão e desconexão, assim como de controle de erro e fluxo fim-a-fim.

3.1.1 Protocolo de transporte orientado à conexão.

Um problema para demonstrar os mecanismos de conexão e desconexão é conhecido como paradoxo dos dois exércitos, mostrado na Figura 3.3.2. O exército Branco (B) está posicionado em um vale e está cercado por duas tropas do exército Azul (A). O fato é que cada tropa do exército Azul é menor que o exército Branco, portanto o exército Azul somente teria sucesso no combate se ambas tropas atacassem simultaneamente o exército Branco. Como o exército Azul pode combinar a data do ataque?

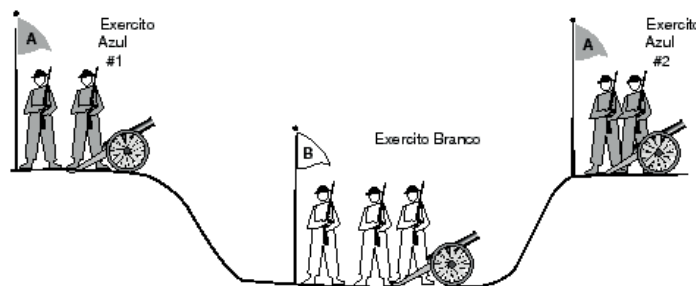



Figura 3.3.2: Paradoxo dos dois exércitos.

A primeira idéia é a tropa #1 enviar um mensageiro para a tropa #2 definindo uma data para o ataque. A tropa #1 não sabe se o mensageiro conseguiu avisar a outra tropa ou se ele foi capturado pelo exército Branco. Se isso ocorresse ele não pode iniciar o ataque porque seria derrotado. Esse exemplo seria de uma comunicação não confiável.

Para melhorar a comunicação, o mensageiro da tropa #1 transmitiria a mensagem para a tropa #2 e retornaria à tropa #1, que confirmaria que a mensagem à tropa #2 foi entregue e confirmada. Assim, a tropa #1 ficaria esperando o retorno do mensageiro para confirmar a recepção correta da mensagem inicial e pudesse atacar na data sugerida. Quando o mensageiro chega à tropa #1, ela agora tem a certeza que pode atacar na data proposta, porém a tropa #2 não teria certeza se o mensageiro chegou à tropa #1 e ficaria em dúvida se iria atacar na data proposta.

Uma terceira proposta seria o mensageiro retornar à tropa #2 para confirmar que a tropa #1 vai atacar na data proposta, com certeza. Mas agora a tropa #1 teria dúvida se a tropa #2 recebeu essa confirmação. Poderíamos ficar trocando mensagens sem fim, e sempre teríamos dúvida se deveríamos ou não atacar na data proposta.

Quando precisamos realizar uma desconexão de uma comunicação encontramos o mesmo problema, basta substituir o termo "atacar" por "desconectar". Por isso chamamos esse problema de paradoxo dos dois exércitos. Como não existe uma solução para esse problema, definimos uma mecanismo de troca de mensagens onde a probabilidade de alguma falha ocorrer é mínima.

Essa mecanismo é chamado handshake de três vias (three-way handshake).

3.2 Protocolo UDP (User Datagram Protocol)

O protocolo UDP provê um serviço sem conexão não confiável, usando IP para transportar mensagens entre duas máquinas. Esse protocolo possibilita que o transmissor possa distinguir fluxo de dados individuais entre múltiplos receptores em uma mesma máquina.

3.2.1 Formato do cabeçalho UDP

A mensagem UDP é formado por um cabeçalho e uma área de dados. O formato do cabeçalho UDP, mostrado na Figura 3.3.3, está dividido em quatro campos de 16 bits.

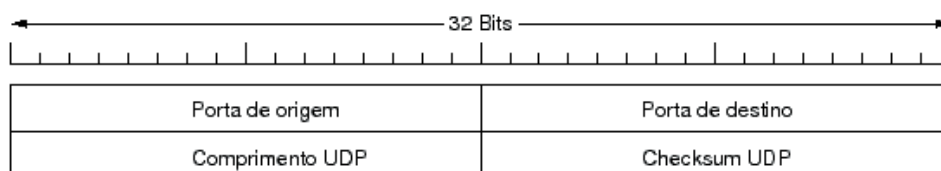



Figura 3.3.3: Formato do cabeçalho UDP.

Definições dos campos:

Porta de origem e destino:

esses campos contêm os números de portas de origem e destino do protocolo UDP. A porta de origem é opcional e é usada para especificar a porta a qual uma resposta poderia ser enviada.

Comprimento UDP:

contém um contador de bytes da mensagem UDP. O valor mínimo é oito, isto é, o comprimento do cabeçalho.

Checksum UDP:

Esse campo é opcional e o valor de zero indica que o checksum não é calculado.

3.2.2 Alguns Números de Portas UDP bem Conhecidos

As portas UDP com número até 1024 são chamadas de portas bem conhecidas (well-known ports). A tabela 3.3.1 mostra algumas portas bem conhecidas do protocolo UDP.

Tabela 3.3.1

Portas UDP bem conhecidas	
Porta	**Descrição**
37	Time
53	DNS
69	TFTP
161	SNMP Monitor
162	SNMP Trap

3.3 Protocolo TCP (Transmission Control Protocol)

O TCP é um protocolo da camada de transporte. Ele é um protocolo orientado a conexão, o que indica que neste nível vão ser solucionados todos os problemas de erros que não forem solucionados no nível IP, dado que este último é um protocolo sem conexão. Alguns dos problemas com os que TCP deve tratar são:

- pacotes perdidos ou destruídos por erros de transmissão.
- expedição de pacotes fora de ordem ou duplicados.

O TCP especifica o formato dos pacotes de dados e de reconhecimentos que dois computadores trocam para realizar uma transferência confiável, assim como os procedimentos que os computadores usam para assegurar que os dados cheguem corretamente. Entre esses procedimentos estão:

1. Distinguir entre múltiplos destinos numa máquina determinada.
2. Fazer recuperação de erros,tais como pacotes perdidos ou duplicados.

Para entender melhor o protocolo TCP a seguir veremos alguns conceitos, para depois passarmos ao formato TCP.

3.3.1 Multiplexação de Conexões TCP

O TCP permite que múltiplos programas de aplicação numa determinada máquina se comuniquem concorrentemente. TCP se encarrega de demultiplexar o tráfego TCP entrante entre os programas de aplicação.

O TCP usa número de portas para identificar o último destino numa máquina. A cada porta é associado um número inteiro pequeno para identificá-lo.

O TCP foi construído sobre a abstração de CONEXÃO, na qual os objetos a serem identificados são conexões de circuitos virtuais e não portas individuais. As conexões são identificadas por um par de “endpoints”. Uma conexão consiste de um circuito virtual entre dois programas de aplicações, então pode-se assumir um programa de aplicação como a conexão entre os endpoints, mas isto não é certo, TCP define um endpoint como um par de inteiros (host, port), onde host é o endereço IP para um computador e Port é uma porta TCP nesse computador.

Exemplo: 128.10.2.3.25 especifica a porta TCP número 25 na máquina como o endereço IP 128.10.2.3. Uma conexão está definida por dois endpoints, assim que se há uma conexão entre as máquinas 192.108.104.12 e 144.54.2.99, a conexão deve ser definida pelos endpoints seguintes: (192.108.104.12,1069) e (144.54.2.99,25).

Já que TCP identifica uma conexão por um par de endpoints, um número de porta pode ser compartilhado por múltiplas conexões na mesma máquina.

3.3.2 Controle de Fluxo

O TCP vê o fluxo de dados como uma sequência de bytes, que ele divide em segmentos para a transmissão. Usualmente cada segmento viaja através da Internet com um único datagrama IP.

TCP usa um mecanismo de "sliding window" para resolver dois problemas importantes:

- Transmissão eficiente
- Controle de fluxo.

3.3.3 Formato do cabeçalho TCP

A unidade de transferência entre o software TCP de duas máquinas é chamado um Segmento. Os segmentos são trocados para estabelecer conexões, transferir dados, enviar reconhecimentos e fechar conexões. Dado que TCP usa a técnica de Piggybacking, um reconhecimento viajando de uma máquina A a B pode ir no mesmo segmento de dados que estão sendo enviados de A a B, embora o reconhecimento refere-se a dados enviados da máquina B a A.

O formato do segmento TCP é mostrado na Figura 3.3.4.

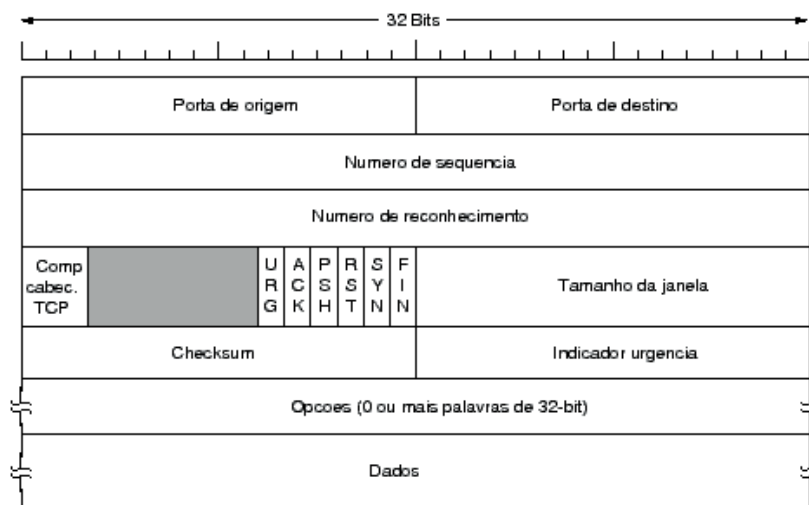



Figura 3.3.4: Formato do cabeçalho TCP.

Definições dos campos do cabeçalho TCP

Porta Origem e Destino:

estes campos no cabeçalho TCP contêm os números de portas TCP que identificam os programas de aplicação dos extremos de uma conexão.

Número de sequência (32 bits):

identifica a posição no fluxo de bytes do segmento enviado pelo transmissor. O número de sequência refere-se ao fluxo de dados que vai na mesma direção do segmento.

Número de Reconhecimento (32 bits):

este campo identifica a posição do byte mais alto (ou último byte) que o fonte recebeu. O número de reconhecimento refere-se ao fluxo de dados na direção contrária ao segmento. Os reconhecimentos sempre especificam o número do próximo byte que o receptor espera receber.

Comprimento cabeçalho TCP

contém um inteiro que especifica o tamanho do cabeçalho TCP, identificando o início do campo de dados. Esse campo é necessário porque o campo de opções tem tamanho variável e o tamanho do cabeçalho TCP varia conforme as opções utilizadas.

Código(6 bits):

determina o propósito e conteúdo do segmento, que é mostrado na tabela 3.3.2.

Tamanho da Janela:

através deste campo o software TCP indica quantos dados ele tem capacidade de receber em seu buffer.

Checksum:

é usado para verificar a integridade tanto do cabeçalho como dos dados do segmento TCP.

Indicador de Urgência:

TCP através deste campo permite que o transmissor especifique que alguns dados são urgentes, isto significa que os dados serão expedidos tão rápido quanto seja possível.

Opções:

campo para opções do protocolo TCP.

Dados:

dados transmitidos pelo usuário.

Tabela 3.3.2

SIGNIFICADO DO CAMPO CÓDIGO DO TCP	
Flag	Significado
URG	Campo de ponteiro Urgente é válido
ACK	Campo de Reconhecimento é válido
PSH	Este segmento solicita um PUSH
RST	Reset da conexão
SYN	Sincroniza números de sequências
FIN	O transmissor chega ao fim do fluxo de dados

3.3.4 Alguns Números de Portas TCP bem Conhecidas

As portas com número até 1024 foram chamadas de portas bem conhecidas (well-known ports). Elas tem aplicação bem específica e são definidas através de RFC. As portas acima de 1024 podem ser utilizadas por qualquer aplicação especial. A tabela 3.3.3 mostra algumas portas bem conhecidas do protocolo TCP.

Tabela 3.3.3

Portas TCP bem conhecidas	
Porta	**Descrição**
20	FTP Data
21	FTP Control
22	SSH
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP-3
443	HTTPS

3.3.5 Máquina de Estados do TCP

A Figura 3.3.5 mostra a máquina de estados finitos do protocolo TCP. O lado esquerdo apresenta os estados relativos à transmissão e o lado direito é relativo à recepção.

O ponto de partida é o estado de repouso (IDLE), localizado na parte superior. Quando uma aplicação deseja iniciar a transmissão ela solicita um comando CONNECT fazendo o protocolo enviar uma mensagem SYN, o que provoca a mudança para o estado WAITING, isto é aguardando o estabelecimento da conexão. Ao receber o ACK o transmissor envia o ACK de confirmação e muda para o estado ESTABLISHED, ou seja, conexão estabelecida. Quando a aplicação solicita o envio de dados o protocolo muda para o estado SENDING, que executa o controle da transmissão de mensagens. No final da comunicação a aplicação solicita o comando de desconexão, fazendo o protocolo mudar para o estado DISCONNECTING, enviando a mensagem FIN. Após a confirmação da desconexão o protocolo retorna para o estado de repouso (IDLE).

No lado de recepção, ao receber uma mensagem de solicitação de conexão (SYN) o protocolo muda para o estado QUEUED. Ao receber o ACK

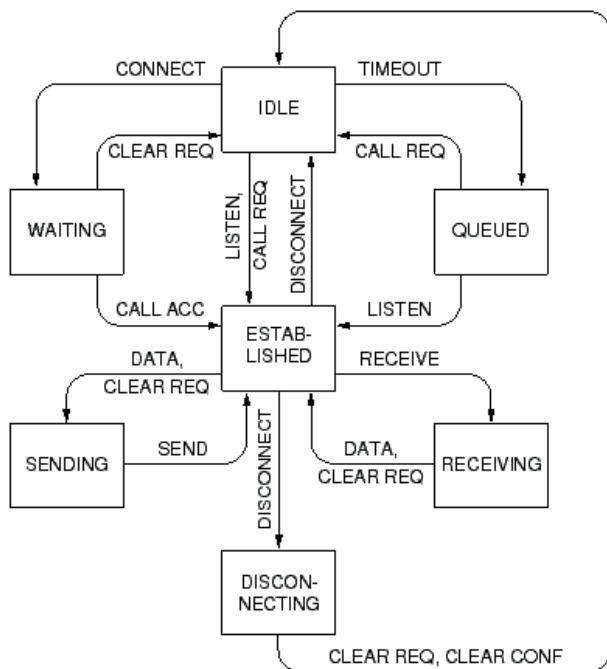



Figura 3.3.5: Máquina de estados do protocolo TCP.

de confirmação muda para o estado ESTABLISHED. Ao receber uma mensagem o protocol muda para o estado RECEIVING, envia o ACK e retorna ao estado ESTABLISHER até o final da comunicação. Ao receber a mensagem FIN, o protocolo muda para o estado DISCONNECTING, que, após o envio do ACK retorna ao estado de repouso (IDLE).

3.3.6 Controle de Congestionamento no TCP

O protocolo TCP implementa vários mecanismos para controlar o congestionamento. A ideia é que transmissor envie a maior quantidade de pacotes possíveis, mas em quantidade suficiente para que o receptor possa processar e a rede possa encaminhar. O controle de congestionamento é dividido em 4 etapas, conforme mostrado na Figura 11.6. Essa figura mostra o tempo, em unidade de tempo de viagem RTT, no eixo X e tamanho da janela em KB no eixo Y.

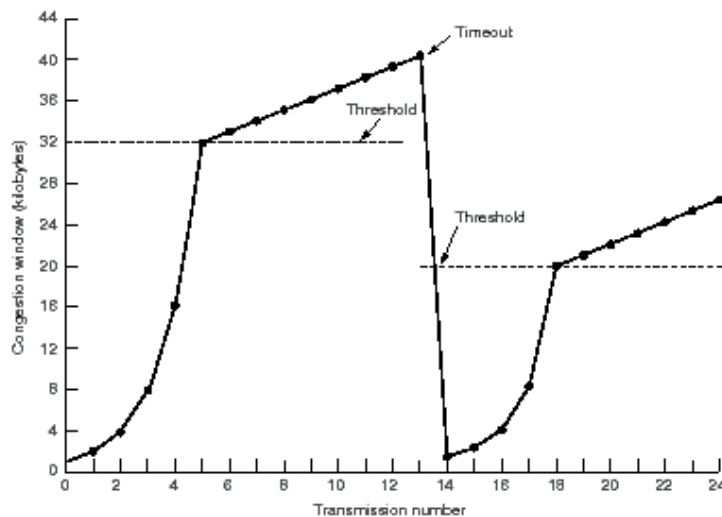



Figura 3.3.6: Controle de congestionamento do protocolo TCP.

A primeira etapa é chamada de Partida-lenta (Slow-start). Nessa etapa, que ocorre logo no início da transmissão, iniciamos a janela com tamanho 1 KB e aumentamos esse tamanho exponencialmente a cada recebimento de reconhecimento (ACK). O nome "Partida-lenta" não é muito adequado, pois o crescimento exponencial seria melhor denominado "Partida-Rápida", porém por razões históricas foi mantido. Esse crescimento ocorre até se atingir o tamanho Limite, previamente configurado, quando passamos para a segunda etapa.

Partida-lenta (Slow-start), Etapa do controle de congestionamento do TCP que ocorre no início da conexão quando a janela de congestionamento inicia com um valor mínimo e aumenta exponencialmente a cada RTT até atingir um valor Limite.

A segunda etapa é chamada Controle de congestionamento (Congestion avoidance). A principal diferença para a Partida-lenta é que o aumento do tamanho da janela se dá de forma linear, aumentando uma janela a cada RTT. O crescimento é mais lento porque se supõe que o TCP está atingindo a capacidade da conexão. Essa etapa ocorre até haver perda de um segmento, seja por timeout ou recebimento de um ACK duplicado, quando passamos para a terceira etapa.

Controle de congestionamento (Congestion avoidance), Etapa do controle de congestionamento do TCP que ocorre após a etapa Partida-lenta e a partir do valor Limite quando a janela de congestionamento aumenta linearmente a cada RTT.

A terceira etapa é chamada Retransmissão rápida (Fast retransmition). Quando o timeout do transmissor expira ou recebe o terceiro ACK duplicado é indicação que a capacidade da rede foi atingida, exigindo uma redução no tamanho da janela. É importante observar que quando o receptor TCP recebe um segmento fora de ordem (indicando que um segmento foi perdido ou está atrasado) ele reconhece o último segmento corretamente recebido, o que provoca o recebimento de reconhecimentos duplicados no transmissor. Geralmente o transmissor recebe reconhecimento duplicado antes de expirar o seu timeout. Quando um desses eventos ocorre a janela é reduzida para o tamanho mínimo e o Limite do tamanho da janela é reduzido para a metade do tamanho da janela corrente. Nesse ponto inicia-se a quarta etapa.

Retransmissão rápida (Fast retransmition) Etapa do controle de congestionamento do TCP que ocorre após a etapa de Controle de congestionamento, quando ocorre um timeout ou reconhecimento duplicado provocando que a janela de congestionamento reduza para o valor mínimo e o valor do Limite seja reduzido para metade da janela corrente.

A quarta etapa é chamada de Recuperação rápida (Fast recovery). Essa etapa aumenta o tamanho da janela exponencialmente até o Limite, quando passa a aumentar linearmente, entrando na etapa de (Congestion avoidance). Essa etapa é muito semelhante à Partida-lenta, porém ela desconsidera os reconhecimentos duplicados que recebe, ainda decorrente da perda do segmento que o fez entrar na etapa de Retransmissão rápida. Se fosse utilizado o algoritmo Partida-lenta original, haveria seguidas reduções do tamanho da janela e do Limite, degradando o desempenho do protocolo.

Recuperação rápida (Fast recovery), Etapa do controle de congestionamento do TCP que ocorre após a etapa de Retransmissão rápida, quando o tamanho da janela aumenta exponencialmente até um valor Limite, que faz entrar na etapa de Controle de congestionamento.

Atividades de avaliação

1. Para que serve uma porta no protocolo de transporte? É necessário uma porta associada ao endereço de origem? Explique.
2. O protocolo UDP oferece um serviço não confiável e orientado à datagrama, semelhante ao serviço oferecido pelo protocolo IP. O protocolo UDP não oferece nenhum serviço adicional, apenas provoca queda no desempenho. Por que uma aplicação não usa diretamente a camada IP sem o protocolo UDP?
3. Descreva e explique as etapas do controle de congestionamento do protocolo TCP.

4. Aplicação

A camada de aplicação oferece para o usuário (ou aplicativo que utiliza a rede para se comunicar) uma interface que implementa os serviços da aplicação, já considerando que oa protocolos inferiores já garante a confiabilidade requerida. Para o usuário comum os serviços de aplicações são os mais conhecidos. A seção 12.1 apresenta a aplicação DNS, a seção 12.2 mostra a aplicação Web, a seção 12.3 apresenta a aplicação de Correio Eletrônico (e-mail), a seção 12.4 mostra a aplicação FTP, e, finalmente, a seção 12.5 apresenta a aplicação Telnet.

4.1 Domain Name System (DNS)

4.1.1 Introdução

Em sistemas distribuídos nomes são utilizados para se referir a uma grande variedade de recursos do sistema, como computadores, portas, serviços e outros objetos do sistema. Tais nomes são necessários para a comunicação entre componentes do sistema e para compartilhamento de recursos. Apresentamos a seguir alguns conceitos importantes.

Serviços de nomes

Permite a ligação de um nome a um conjunto de atributos relacionados

a este nome. A mais frequente operação que é solicitada a um serviço de nomes é a resolução de um nome, i.e.,a procura dos atributos relacionados a um determinado nome.

Espaço de nomes

É uma coleção de nomes sintaticamente válidos reconhecidos por um sistema de resolução de nomes. Ex.: /usr/home em sistema de arquivos Unix.

Contextos

A resolução de um determinado nome nem sempre se dá de maneira direta, isto é, não solicitamos ao serviço de nomes a simples resolução de um nome absoluto (plano). Geralmente o nome é identificado dentro de um contexto. Um contexto funcionaria de maneira análoga ao sistema de diretório: um diretório definiria um contexto para para a resolução dos nomes. Assim: /home/jose/arquivo1 (a) /home/maria/arquivo1 (b) O nome arquivo1, quando apresentado ao serviço de resolução de nomes com o contexto /home/jose retornaria uma referência ao objeto do sistema indicado por (a) que, não necessariamente, seria o mesmo objeto que (b). Como podemos ver um mesmo nome pode aparecer em contextos diferentes referenciando objetos diferentes.

Um serviço de nomes que não permite a definição de mais que um contexto para o seu espaço de nomes é dito possuir um espaço de nomes flat. Para um espaço de nomes flat existe somente um único contexto. De volta a nossa analogia com o sistema de diretório, um sistema flat seria um sistema de diretório que só possuísse um único diretório: o raiz. Neste caso, todos os nomes são resolvidos de maneira global, absoluta, sempre em relação ao único contexto existente.

Domínio de Nomes

É um espaço de nomes para o qual existe uma única e geral autoridade administrativa. Esta autoridade determina quais nomes podem ser inseridos/removidos dentro de seu espaço de nomes.

Resolução de Nomes

Em geral, a resolução de um nome é um processo iterativo em que um nome é apresentado repetidas vezes a diferentes contextos de nomes. Assim para resolvermos o nome/home/jose/arquivo1, teríamos os seguintes passos:

- Apresentamos o nome /home/jose/arquivo1 ao sistema.
- O nome home é resolvido então no contexto raiz, retornando um

identificador válido, ou então uma condição de erro.

- Caso o valor de retorno seja um identificador válido, apresentamos o nome jose ao contexto /home.
- Novamente, se o valor de retorno for um identificador válido, prosseguimos com a resolução de nosso nome. Apresentamos arquivo1 ao contexto /home/jose e, finalmente, nos é retornado um identificador (ou outro atributo) para o nome /home/jose/arquivo1.

4.1.2 Histórico

Divisão do espaço de nomes em contextos. Inicialmente, o espaço de nomes da Internet era flat e administrado por uma única entidade centralizadora, responsável pelo único contexto então existente. Como o número de nomes cresceu muito, ficou impossível para tal entidade administrar um espaço de nomes gigantesco, bem como prestar serviços a todos os demais usuários. Surgiu então o DNS, um sistema de resolução de nomes distribuído, onde existiam vários domínios: subespaços de nomes administrados localmente.

Assim, por exemplo, uma universidade americana era responsável pelo seu domínio, podendo ela determinar a inclusão e remoção de nomes de seu espaço de nomes, bem como incumbida de ajudar na solução de nomes que referissem a um dos contextos pertencentes a seu domínio. Todo domínio possui uma única autoridade sobre as operações de pesquisa e atualização de seu espaço de nomes.

4.1.3 Domínio

Como posso mandar uma carta para você? Este tipo de pergunta resulta numa resposta do tipo: Rua, Número, Bairro, Cidade, Estado, País e um Número (CEP) para facilitar a identificação do logradouro, para envio de cartas sem contar com o seu nome que aparece na carta. Para que você possa comunicar com outro usuário existe também um endereço eletrônico; assim sendo a estrutura apresentada para endereços é: Usuário@domínio.

O domínio pode ser dividido em várias partes chamadas subdomínios. Estas partes estarão separadas por ponto (".") Assim se tivessem o seguinte endereço eletrônico: joao@servidor.empresax.com.br.

O subdomínio mais à direita é o domínio de maior nível, conforme você ler os subdomínios mais à esquerda eles tornarão mais específicos o possível; O domínio de maior nível indica em que país se encontrará, a ausência do domínio de maior nível, indica que a máquina estará no EUA (isto é obvio, foi aonde iniciou-se a Internet). No nosso caso o domínio de maior nível é br (Brasil).

Redes de Computadores_NL2014.indd 170 02/05/2019 17:10:18

O subdomínio seguinte define o tipo de instituição ao qual pertence. No nosso exemplo com define um domínio comercial (pertencente a uma empresa). Veja na tabela os tipos de subdomínio padronizados. O próximo subdomínio empresax seria a indicação da empresa que mantém este endereço eletrônico e o último subdomínio servidor seria o nome de uma máquina específica que a empresa mantém onde reside o programa de e-mail. Você poderá ver domínios divididos em mais de 3 subdomínios porém, não existem na Internet domínios divididos em menos de 2 subdomínios.

4.1.4 DNS

Imagine agora a sua necessidade de se comunicar com uma máquina ou com um usuário. Como sabemos os computadores trabalham com números e nós não somos capazes de decorar todos os números possíveis. Um exemplo 197.168.8.30, 149.82.34.11, 149.82.34.4, deste modo fica difícil saber onde estão estas máquinas (se no Brasil ou no Exterior).

Por isso foi criado o FQDN, ou seja, Nome do Domínio Completamente Qualificado, ou mais conhecido como DNS. Assim, o número 197.168.8.30 é da máquina server.empresax.com.br, o endereço 149.82.34.11 é da marte.escola.edu.br, o endereço 149.82.34.4 é da venus.escola.edu.br, agora ficou mais fácil pois vemos que o primeiro endereço é de uma máquina na empresax e os outros dois são de máquinas da escola.

Esses números IPs são aleatórios usados apenas para exemplificar, pedimos desculpas se eles correspondem à máquinas reais.

O último domínio indicará o país em que esta máquina esta situada, o segundo domínio indica a instituição que detêm o domínio e o primeiro nome indica uma máquina, ou mais especificamente, um endereço IP, o que chamamos de Endereços Internet Protocol (IP). Os IP's são constituídos por quatro números unidos por pontos ('.') chamados de quádrupla ou dottedquad e cada pedaço deste número é chamado de octeto. As informações na rede são passadas pelo números IP's e não pelo FQDN. O programa DNS faz todo o "trabalho árduo" para passar de FQDN para IP ou de IP para FQDN.

4.2 World Wide Web (WWW)

O WWW (World Wide Web), é o maior aplicativo existente na Internet. Sua facilidade de uso e simplicidade permitiram o grande crescimento da Internet no mundo. De fato é tedioso utilizar serviços como FTP, Telnet, conhecer e aprender todos os requisitos e comandos. Com o acesso a WWW você pode escolher o que pesquisar, sem muitas complicações e sem ao menos saber em que local da rede ele se encontra, o WWW utiliza o método de Hipertextos, são textos que em certas palavras podemos "clica-las" e assim navegando-se dentro da rede, podendo salvar telas, imprimi-las, copiar programa, ou seja, é um dos estágios

finais de aglutinação de tudo o que é possível fazer e se obter dentro da rede.

O WWW teve início no CERN (Centre Europeene Recherche Nucleaire), a ideia era padronização de tudo o que é possível conectar-se à rede Internet, podendo assim utilizara rede como um todo e um enorme banco de dados, com a existência de vários tipos de dados,daí a sua implementação ao suporte de multimídia. Foi então criado o protocolo HTML (Hyper Text Mark-up Language) e os dados em relação a um servidor e cliente como HTTP (Hyper TextTransfer Protocol).

A ideia é utilizar páginas com textos, imagens e ícones fazendo com que da combinação destes elementos, obtenhamos uma tela visível, com as opções de mover-se entre estas páginas. Resumindo, seria como se você tivesse virando folhas de um livro.

Normalmente utilizamos um software específico chamado de cliente WWW ou Navegador (browser). Como exemplo, podemos destacar o Mozilla, o Opera, o Chrome, o Internet Explorer, dentre outros. Existem implementações para qualquer plataforma seja ela PC Windows, MAC ou o ambiente XWindows do UNIX.

Os componentes do modelo Web são mostrados na Figura 3.4.1.

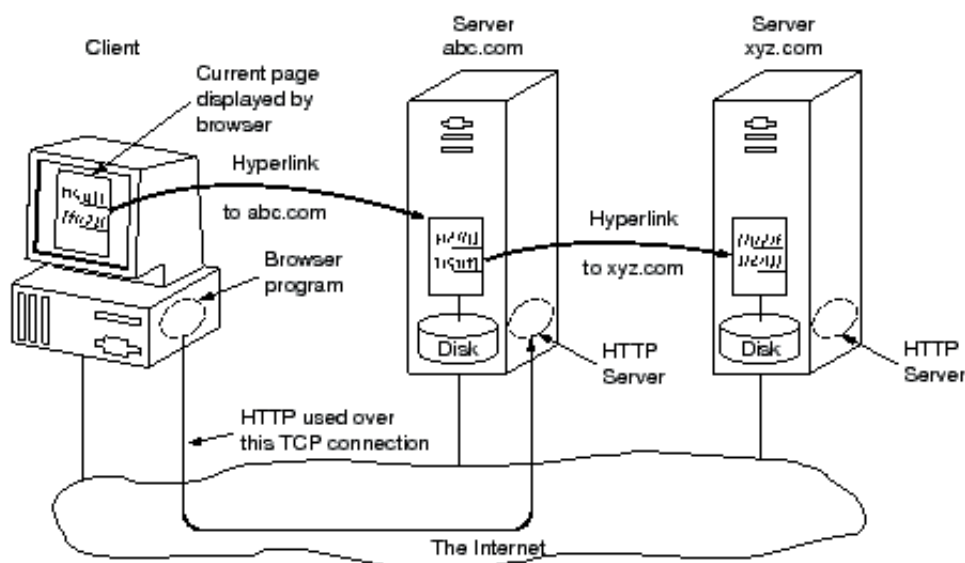



Figura 3.4.1: Componentes do Modelo Web.

4.2.1 Protocolo HTTP (Hypertext Transfer Protocol)

O protocolo HTTP é um protocolo do nível de aplicação que possui objetividade e rapidez necessárias para suportar sistemas de informação distribuídos, cooperativos e de hipermídia. Suas principais características são as seguintes:

- propiciam busca de informação e atualização
- as mensagens são enviadas em um formato similar aos utilizados pelo correio eletrônico da Internet e pelo MIME (Multiporpose Internet Mail Extensions)
- comunicação entre os agentes usuários e gateways, permitindo acesso a hipermídia a diversos protocolos do mundo Internet, tais como, SMTP, NNTP, FTP, etc
- pode ser implementado em cima de qualquer protocolo Internet
- obedece ao paradigma de pedido/resposta: um cliente estabelece uma conexão com um servidor e envia um pedido ao servidor, o qual o analisa e responde. A conexão deve ser estabelecida antes de cada pedido de cliente e encerrada após a resposta.

As mensagens seguem o formato da RFC822 e se apresentam na forma de:

- Pedidos enviados pelo cliente ao servidor
- Respostas enviadas pelo servidor para o cliente

4.2.2 Métodos

Método indica a forma a ser aplicada para requisitar um recurso. Os métodos aceitos por um determinado recurso podem mudar dinamicamente. O cliente é notificado com o código 501quando o método é desconhecido ou não implementado. Os métodos são sensitivos ao caso. Os principais métodos são:

GET Recupera todas as informações identificadas no recurso da rede. Se o recurso for um processo executável, ele retornará a resposta do processo e não o seu texto. Existe o **GETcondicional** que traz o recurso apenas se o mesmo foi alterado depois da data da última transferência. **HEAD** Semelhante ao método GET, só que neste caso não há a transferência da entidade para o cliente. Este método é utilizado para testar a validade e acessibilidade dos links de hypertexto. **POST** Utilizado para solicitar que o servidor destino aceite a entidade constante no pedido como um novo subordinado ao recurso constante no URI. Suas principais funções são:

1. anotações de recursos existentes
2. postar uma mensagem em um bulletin board, newsgroup, mailing list
3. abastecer um processo com um bloco de dados
4. extender uma base de dados com uma operação de append

A entidade é subordinada da mesma forma que um arquivo é subordinado ao diretório, o registro a base de dados PUT Coloca a entidade abaixo do recurso especificado no pedido. Se esta entidade não existe é criada. Se existe,

apenas é atualizada DELETE Solicita que o servidor origem apague o recurso identificado no URI LINK Estabelece uma ou mais relações de links entre o recurso identificado pelo URI e outros recursos existentes, não permitindo que o corpo da entidade enviada seja subordinada ao recurso UNLINK Remove uma ou mais relações de links existentes entre o recurso identificado no URI.

URI (Uniform Resource Identifiers)

URI identifica o recurso da rede. Por exemplo:

server.escola.edu.br/pub/rfc/rfc822.txt

Quando o caractere "*" aparece antes do recurso da rede, o mesmo indica que a requisição não se aplica ao recurso de rede especificado e sim ao seu servidor.

4.2.3 Cabeçalhos

O pedido possui três cabeçalhos distintos:

- Cabeçalho Geral São dados complementares não relacionados com as partes que estão se comunicando nem com o conteúdo sendo transferido. Exemplo: data, versão do MIME.
- Cabeçalho de Resposta Informações adicionais sobre o pedido e o cliente, como por exemplo, o intervalo de respostas esperadas no processamento da requisição.
- Cabeçalho da Entidade Informações adicionais sobre a entidade, tais como: título da entidade, tamanho, linguagem utilizada.

4.2.4 Códigos de Resposta

O status representa o resultado do processamento executado pelo servidor. O status possui o seguinte formato: 9XX, onde, 9 representa a classe da resposta e XX representa a categoria da resposta.

Atualmente o protocolo possui cinco classes de respostas:

1XX

Não utilizada, reservada para utilização futura

2XX Sucesso:

a ação foi recebida, entendida e executada com sucesso. Com o método GET, a entidade correspondente é enviada com a resposta. Com o método HEAD, a resposta contém o cabeçalho da informação. Com o método POST, a resposta descreve/contém o resultado da ação. Nos restantes, a resposta descreve o resultado da ação. Exemplos:

201 - Um novo recurso foi criado

202 - O pedido foi aceito para processamento, mas o mesmo não foi concluído

3XX Redirecionamento:

indicam que as ações devem ser efetuadas em ordem para completar o pedido. Exemplos:

300 - O recurso requisitado está disponível em mais de um local e o local preferido não pode ser determinado via negociação

302 - O recurso requisitado reside temporariamente em outro URI

4XX Erro no cliente:

pedido contém erro de sintaxe ou não pode ser efetuado. Exemplos:

401 - O recurso requisitado necessita autenticação do usuário

404 - O servidor não encontrou o recurso definido no URI

5XX Erro no servidor:

o servidor falhou ao executar um pedido aparentemente válido. Exemplos:

500 - Erro interno no servidor

501 - Recurso solicitado não implementado no servidor

4.3 Correio Eletrônico (Electronic Mail ou E-Mail)

A troca de correspondência eletrônica é o segundo recursos mais utilizado na Internet. Como em cada máquina existe um programa diferente que controla suas cartas, estes programas além de usar o mesmo protocolo TCP/IP, devem receber, enviar, reenviar, salvar, imprimir e apagaras cartas lidas. Apresentaremos apenas os comandos genéricos, existentes em qualquer programa.

Um e-mail é semelhante a uma carta escrita em papel. Uma carta é constituída por um envelope e um conteúdo (a carta propriamente dita). O e-mail tem um “envelope” que contém o nome e endereço do destinatário, o nome e endereço do remetente e uma linha opcional para escrever o assunto. O conteúdo é onde escrevemos a carta, e geralmente é como um editor de textos.

O nome e endereço é simplesmente o endereço padrão Internet, isto é, nome@domínio. Somente com essa sigla podemos identificar o destinatário e o rementente. Geralmente o endereço do remetente é definido no próprio programa de e-mail e não necessita ser escrito quando se envia um e-mail. Também não é necessário datar pois o programa já inclui a hora e data local .

Se quisermos enviar uma carta para o joão que está no endereço empresax.com no Brasil fica assim:

```
Mail to: joao@empresax.com.br
```

```
Cc:

Subject: Saudacoes

Ola’ Joao, como vai?

Abracos,

Maria
```

Observe que acentos da língua portuguesa geralmente não são usados no endereço, pois não são compreendidos por muitos equipamentos (apesar de cada vez mais ser aceito). Além disso, não se deve colocar acentos no texto escrito, mesmo que o programa de e-mail permita. Alguns equipamentos na Internet (por exemplo, proxies), não entendem os caracteres ASCII estendidos, e trocam os caracteres acentuados por outros caracteres que poderão tornar o e-mail incompreensíveis pelo destinatário. Assim, principalmente se for enviar um e-mail para o exterior, é recomendado não colocar acentos.

O campo Cc serve para enviar uma cópia do e-mail para outra pessoa. Neste caso tanto quem receber a mensagem como Mail to ou Cc saberá que o outro recebeu também a mensagem. Alguns programas também apresentam um campo Bcc, de Blind Copy ou cópia secreta, que indica uma pessoa que receberá o e-mail, sem que as outras, Mail to e Cc, saibam que ela recebeu uma cópia.

O João receberá a seguinte mensagem quando ele conectar o computador à Internet.

```
Subject: Saudacoes
Date: Sun, 10 Jun 2007 12:34:22 -0745
From: maria@escola.edu.br
To: joao@empresax.com.br

Ola’ Joao, como vai?

Abracos,

Mario
```

Se João quer responder o e-mail ele simplesmente clica em Reply. Esse comanda copia o endereço do remetente para ser destinatário de um novo e-mail e, se ele quiser, copia acarta recebida. Para indicar quais partes foram copiadas do e-mail original é colocado o sinal “>”na frente de cada linha copiada. Se esta mensagem sofrer outro reply serão colocados “>”na frente, de tal forma que podemos saber a sequência de envio de mensagem.

```
> Subject: Saudacoes
> Date: Sun, 10 Jun 2007 12:34:22 -0745
> From: maria@escola.edu.br
> To: joao@empresax.com.br
>
> Ola' Joao, como vai ?
>
> Abracos,
>
> Mario
>

Ola' Maria,

Tudo bem comigo. E voce ?

Joao
```

Se João além de responder para Mario quiser enviar uma cópia para outra pessoa, ele pode usar o comando Forward, isto é, encaminhe para.

4.3.1 SMTP (Simple Mail Transfer Protocol)

Permite enviar, receber e armazenar mensagens eletrônicas para usuários de outros computadores (correio), observando os endereços eletrônicos.

O programa de e-mail na máquina do usuário abre a conexão para o servidor de e-mail. O programa dá o nome da máquina, o remetente e o conteúdo da mensagem. Então envia um comando dizendo que está iniciando a mensagem neste ponto, o outro lado termina o tratamento que é visto como comando e começa a receber a mensagem. A ponta remetente começa então a enviar o texto da mensagem.

No final, uma marca especial é enviada. Após isto, ambas as pontas compreendem que aponta remetente está novamente enviando comandos.

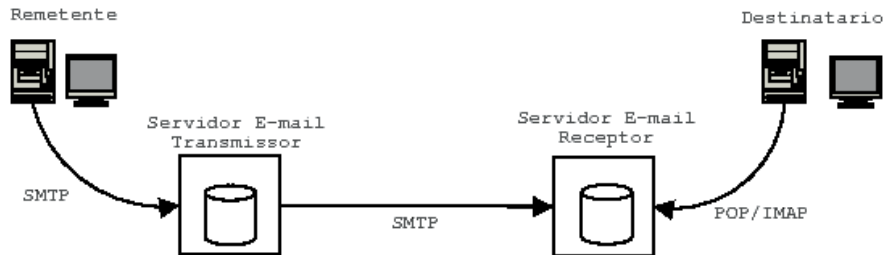



Figura 3.4.2: Componentes de um sistema de correio eletrônico.

Na Figura 3.4.2 o usuário chama a "interface de usuário" para depositar ou recuperar e-mails, todas as transferências são em background, isto é, sem a necessidade de intervenção do usuário.

Comunicação entre cliente e servidor:

1. cliente estabelece conexão com servidor e espera o servidor enviar a mensagem 220 READY FOR MAIL
2. após, cliente envia o comando HELO, o fim da linha marca o fim do comando
3. o servidor responde identificando-se
4. com a conexão estabelecida, o remetente pode transmitir uma ou mais mensagens de e-mails, terminar a conexão, ou solicitar que o servidor troque as regras de enviar e receber, assim, mensagens podem fluir na direção oposta.
5. a transmissão começa com o comando mail que dá a identificação do remetente
6. a partir do comando DATA, o receptor responde com a mensagem "start mail input"

Exemplo: Smith deseja mandar uma mensagem para Jones (s - servidor, c - cliente)

```
s: 220 escola.edu.br SMTP ready
c: HELO empresax.com.br
s:250 escola.edu.br
c: mail from:<@escola.edu.br>
s:250 ok
c: RCPT to:<@empresax.com.br>
s:250 ok
```

```
c: DATA
s:354 start mail input; end with
<><>.<><>
c: .... envia mensagens de mail....
c: ..... mensagens....
c: <><>.<><>
s: 250 ok
c: QUIT
s: 221 beta.gov service closing trans-
mission channel Enviar uma mensagem
   para o usuario joao, no computador
empresax.com.br, observando o
   formato da mensagem :
% Mail joao@empresax.com.br
subject: Saudacoes

Ola’ Joao, como vai?

Abracos,

Maria

^d
```

Características

Possui basicamente três entidades: Agente do Usuário, Emissor-SMTP e Receptor-SMTP.

- É orientado a conexão, sendo transmitido sobre TCP.
- A comunicação entre Emissor-SMTP e Receptor-SMTP é feita através de comandos formados por sequências de caracteres no padrão ASCII.
- Apenas alguns dos comandos tem implementação obrigatória em um servidor básico: HELO, MAIL, RCPT, DATA, NOOP, QUIT e RSET
- Para cada comando enviado do Emissor-SMTP para o Receptor-SMTP ocorerá uma resposta do Receptor, através de um Código Numérico de Resposta.

Funcionamento Básico

É estabelecido a conexão entre Emissor-SMTP e Receptor-SMTP, onde este último pode ser o destino final da mensagem ou apenas um retransmissor.

1. O Emissor-SMTP envia a identificação do Remetente da mensagem, que o Receptor-SMTPresponde com um OK.
2. Após, identifica-se o destinatário da mensagem, então, o Receptor--SMTP verifica see ste existe e retorna o código apropriado.
3. Estando identificado o destinatário o Emissor-SMTP começa o envio da mensagem propriamente dita.
4. Ao seu término o Emissor-SMTP envia um sequência especial de finalização.
5. Então, a conexão entre o Emissor-SMTP e o Receptor-SMTP é desativada.

4.3.2 Comandos SMTP

Semântica dos Comandos

```
HELO <SP> <domain> <CRLF>
MAIL <SP> FROM:<reverse-path> <CRLF>
RCPT <SP> TO:<forward-path> <CRLF>
DATA <CRLF>
RSET <CRLF>
SEND <SP> FROM:<reverse-path> <CRLF>
SOML <SP> FROM:<reverse-path> <CRLF>
SAML <SP> FROM:<reverse-path> <CRLF>
VRFY <SP> <string> <CRLF>
EXPN <SP> <string> <CRLF>
HELP [<SP> <string>] <CRLF>
NOOP <CRLF>
QUIT <CRLF>
TURN <CRLF>
```

Descrição dos Comandos

HELO

(HELLO) (Obrigatório) Identifica o Emissor da mensagem para o Receptor.

MAIL

(Obrigatório) Este comando inicializa uma transação de mail na qual uma mensagem é enviada a uma ou mais caixa de mensagens (mailbox).

RCPT

(ReCiPienT) (Obrigatório) Este comando identifica o destinatário da mensagem;múltiplos destinatários são definidos por múltiplos usos desse comando.

DATA

(Obrigatório) Inicializa a transmissão da mensagem, após seu uso é transmitido o conteúdo da mensagem, que pode conter qualquer um dos 128 caracteres ASCII. O seutérmino é especificado por uma sequência "<CRLF>.<CRLF>".

RSET

(ReSET) (Obrigatório) Este comando determina que a operação atual de e-mail deverá ser abortada. Todos os dados referentes são descartados.

SEND

Este comando é usado para inicializar uma transação de e-mail na qual uma mensagem é enviada para um ou mais terminais onde estejam os destinatários e não para os seus mailboxes. É um comando alternativo ao comando MAIL

SOML

(Send Or MaiL) Este comando é usado para inicializar uma transação de e-mail na qual uma mensagem é enviada para um ou mais terminais onde estejam os destinatários ou aseus mailboxes. A mensagem é direcionada aos terminais dos destinatários ativos no momento(e aceitando mensagens) caso contrário é direcionada aos seus mailboxes. É alternativo ao comando MAIL.

SAML

(Send And MaiL) Este comando é usado para inicializar uma transação de e-mail na qual uma mensagem é enviada para um ou mais terminais dos destinatários e aos seus mailboxes. A mensagem é direcionada aos terminais dos destinatários ativos no momento (e aceitando mensagens) e a todos os mailboxes.

VRFY

(VeRiFY) Este comando solicita ao Receptor-SMTP a confirmação de que o argumento identifica um usuário conhecido. Se for identificado é retornado o nome completo do usuário (se este possuir) e seu mailbox completo.

EXPN

(EXPaNd) Este comando solicita ao Receptor-SMTP a confirmação de que o argumento identifica uma lista de usuários de e-mail (mailing list). Se

for identificada serão retornados os membros desta lista no mesmo formato retornado pelo comando VRFY.

HELP

Este comando faz com que o Receptor-SMTP envie informação de ajuda ao Emissor-SMTP.

NOOP

(Obrigatório) Este comando não possui efeitos nem parâmetros. Apenas faz com que o receptor envie um OK.

QUIT

(Obrigatório) Este comando determina que o Receptor-SMTP envie um OK e então feche o canal de comunicação com o Emissor-SMTP.

TURN

Este comando faz com que o Receptor e o Emissor troquem de papéis, o Receptor fica como Emissor e o Emissor como Receptor.

4.3.3 Códigos de Resposta

211 System status, or system help reply

214 Help message (Informação de como usar o Receptor-SMTP ou algum comando nãopadronizado)

220 <domain> Service ready

221 <domain> Service closing transmission channel

250 Requested mail action okay, completed

251 User not local; will forward to <forward-path>

354 Start mail input; end with <CRLF>.<CRLF>

421 <domain> Service not available, closing transmission channel (É uma resposta que pode ser dada a qualquer comando; indica que a conexão foi desfeita)

450 Requested mail action not taken: mailbox unavailable (Ex.: maixbox está em uso)

451 Requested action aborted: local error in processing

452 Requested action not taken: insufficient system storage

500 Syntax error, command unrecognized (Usado também para casos tal como linha muito longa)

501 Syntax error in parameters or arguments

502 Command not implemented

503 Bad sequence of commands

504 Command parameter not implemented

550 Requested action not taken: mailbox unavailable (ex.: mailbox não encontrado, sem acesso)

551 User not local; please try <forward-path>

552 Requested mail action aborted: exceeded storage allocation

553 Requested action not taken: mailbox name not allowed (ex.:sintaxe do mailbox errada)

554 Transaction failed

4.4 File Transfer Protocol (FTP)

4.4.1 Utilização do FTP

Volta e meia precisamos de um programa para nossas máquinas, tal como, um novo anti-vírus, uma fonte para Word, ou seja, versões atualizadas de programas ou novos programas. Para isso existe o serviço FTP, onde podemos pegar estes programas em vários lugares no mundo. Usaremos o comando FTP mais o local em que faremos a busca, utilizaremos o serviço do servidor.com.br.

1º Digita-se:

Ñí é =ë Éê î á Çç ê KÅç ã KÄê

Isto vai gerar algo do tipo: connected to servidor.com.br

å ~ã ÉW

2º Entre com o login:

å ~ã ÉW=~å ç å ó ã ç ì ë

é ~ë ë ï ç ê ÇW

3º Entre com a senha, que pode ser qualquer uma, mas vamos usar o nosso e-mail: joao@empresax.com.br

å ~ã ÉW=~å ç å ó ã ç ì ë

é ~ë ë ï ç ê ÇW=ñ ñ ñ ñ ñ ñ ñ ñ ñ ñ ñ ñ ñ ñ ñ ñ ñ ñ ñ

OP M=~å ç å ó ã ç ì ë =ä ç ÖÖÉ Ç=á å

4º Repare que estamos agora na máquina remota que é um servidor Unix. Então vamos vamos tentar o comando "ls" para listar o diretório.

Ñí é [=ä ë

OMM=mç ê í =Åç ã ã ~å Ç=ë ì ÅÉë ë Ñì ä K

NRM=éÉåáåÖ=p`ff=ãçÇÉ=€~í~=Âçåå ÉÅíáçå=Ñçê=Ñáä É=äáëí

Çêï Çêï J êï NMOQl Åí =NR=NOWMM=K

Çêï Çêï J êï NMOQl Åí =NR=NOWMMKK

Çêï Çêï J êï NMOQ=kçî =OP=NPWOQ=éìÄ

J êï J ê J ê J NMRSM=aÉÅ=NN=NNWRM=äÉá~ãÉKíñí

OOS=qê~åëÑÉê=`çãéäÉíÉ

PONU=_óíÉë=êÉÅÉáîÉÇ=NKO=ëÉÅçåÇë=EOKS=hÄLëF

Ñíé[=

Repare que onde existe a letra “d” é um diretório. O nome do diretório está na última coluna, os dois primeiros não são diretório, são do sistema (o mesmo tipo que existe numa máquina Unix convencional). O PUB é um diretório, normalmente este onde encontraremos os arquivos do nosso interesse. O leiame.txt é um arquivo, repare na 1º coluna “-” (pode também ser “a”) indica que é um arquivo. Suponha que primeiramente você queira saber o que tem dentro deste arquivo leiame.txt, basta enviar para a sua máquina(lembre-se que no momento é como se você estivesse lá).

5º Então deve usar o comando get da seguinte forma: get leiame.txt. Lembre-se você está numa máquina Unix, então se comporte como se estivesse usando uma:

Ñíé[=ÖÉí =äÉá~ãÉKíñí

OMM=mçêí=Åçãã~åÇ=ëìÅÅÉëëÑìä

NRM=éÉåáåÖ=p`ff=ãçÇÉ=€~í~=Âçåå ÉÅíáçå=Ñçê=äÉá~ãÉKíñí =ENMRSM=_óíÉëF

OOS=qê~åëÑÉê=Åçãéä Éí É

RM=_óíÉë=êÉÅÉáîÉÇ=SKV=ëÉÅçåÇë=ENKMQT=hÄLëF

Ñíé[

6º Agora suponha-se que você queira entrar num subdiretório, no caso, no diretório "PUB", basta usar o comando cd pub e de um novo ls, isto vai gerar algo do tipo:

Ñí é [=ÅÇ=é ì Ä

OMM=mç ê í =Åç ã ã ~å Ç=ë ì ÅÅÉë ë Ñì ä

ORM=` t a=Åç ã ã ~å Ç=ë ì ÅÅÉë ë Ñì ä

Ñí é [=ä ë

OMM=mç ê í =Åç ã ã ~å Ç=ë ì ÅÅÉë ë Ñì ä

NRM=é Éå á å Ö=p` f f=ãç ÇÉ=Ç~í ~=Åç å å ÉÅí á ç å=Ñç ê=Ñá ä É=ä á ë í K

Çê ï Çê ï J ê ï NMOQl Åí =NR=NOWMM=K

Çê ï Çê ï J ê ï NMOQl Åí =NR=NOWMMKK

J ê ï J ê J ê J NPQQQk ç î =OP=ONWRM=~ê è ì á î ç NKò á é

J ê ï J ê J ê J NTMT=k ç î =OP=ONWRR=~ê è ì á î ç OKò á é

OOS=q ê ~å ë ÑÉê =Åç ã é ä Éí É

RQNQ=_ó í Éë =ê ÉÅÉá î ÉÇ=NKN=ë ÉÅç å Çë =EQKV=h ÄLë F

Ñí é [

7º Suponha-se que queremos o arquivo arquivo2.zip, note que ele não é um diretório e nem um arquivo texto, portanto para seu melhor modo envio ele tem que ser transferido por conjuntos de byte's.

Devemos usar o comando binary (bin) antes de usar o comando get, para informar que o arquivo que está sendo transferido é binário. Depois da transferência destes arquivos sairemos imediatamente do servidor usando o comando quit.

é ì Ä[=Äá å

OMM= q ó é É = ë É í = í ç = f

é ì Ä[= ÖÉ í = ~ ê è ì á î ç OKò á é

OMM= mç ê í = Åç ã ã ~ å Ç = ë ì ÅÅÉ ë ë Ñì ä

PRP= ë é É å á å Ö= Ä á å ~ ê ó = ã ç ÇÉ= Åç å å ÉÅí á ç å= Ñç ê = ê è ì á î ç OK ò á é ENTMT= _ ó í É ë F

QRS = Äó í É ë = í ê ~ å ë ÑÉ ê
QNN= Äó í É ë = í ê ~ å ë ÑÉ ê
QOO= Äó í É ë = í ê ~ å ë ÑÉ ê
QRS = q ê ~ å ë ÑÉ ê = Åç ã é ä É í É
NTMT= _ ó í É ë = ê ÉÅÉ á î ÉÇ == S KN= ë ÉÅç å Çë = EMKOT= h Ä L ë F

é ì Ä[= è ì á í

OMM= mç ê í = Åç ã ã ~ å Ç = ë ì ÅÅÉ ë ë Ñì ä
OON= Äó É

4.4.2 Principais comandos

ASCII

Alterna para o modo ASCII. O Modo ASCII é o modo default usado para transferência de arquivos textos;

BIN

Alterna para o modo Binary. Para transferência de arquivos binários tipo .exe,.com, .zip entre outros.

CD

Muda de diretório na máquina que você está acessando (O remoto);

DIR ou LIST

Lista os arquivos no diretório corrente do remoto;

GET

Cópia arquivos do micro remoto para a sua conta;

HELP

Mostras os comandos existentes e suas funções;

LCD

Muda de diretório na sua conta corrente (O L é de local);

MGET

Cópia múltiplos arquivos do computador remoto para o seu;

MPUT

Transfere múltiplos arquivos da sua conta para o computador remoto;

PUT

Transfere arquivos da sua conta corrente para a máquina remota (ftp anônimos não aceitam este comando);

O FTP também pode ser utilizado para acessar outra máquina ou conta de outro sistema, caso haja a necessidade de enviar arquivos ou de copiar arquivos de uma máquina ou conta para uma outra máquina e conta, basta saber o FQDN ou IP deste outra máquina o login e o password desta outra conta. É neste caso que podemos utilizar os comandos PUT e MPUT descritos anteriormente.

4.4.3 Protocolo FTP

O FTP é o protocolo de transferência de arquivos da Arquitetura Internet. Trata-se de um utilitário de uso interativo que pode ser chamado por programas para efetuar transferência de arquivos. Os seus principais objetivos são:

- motivar a utilização de computadores remotos;
- tornar transparentes ao usuário diferenças existentes entre sistemas de arquivos associados a estações de uma rede;
- transferir dados de maneira eficiente e confiável entre dois sistemas;
- promover o compartilhamento de arquivos, sejam programas ou dados.

O FTP não se preocupa em definir um sistema de arquivos virtual e sim em definir uma interface com os sistemas de arquivos nativos. Podemos dividir o entendimento do protocolo em quatro partes:

1. Modelo
2. Sistema de Arquivos
3. Processo de Transferência de Arquivos
4. Comandos.

Modelo

O FTP trabalha com o modelo CLIENTE-SERVIDOR. O modelo implementado possui uma característica interessante, que é a de utilizar duas conexões diferentes entre os sistemas envolvidos: uma denominada conexão

de controle, dedicada aos comandos FTP e suas respostas, e a outra denominada conexão de dados, dedicada à transferência de dados.

A parte executada no cliente (chamada de Cliente-FTP) pode ser dividida em três módulos que interagem por algum mecanismo interno. Esses módulos são:

1. Interface do Usuário
2. Interpretador de Protocolo do Cliente (Cliente-PI)
3. Processo de Transferência de dados (Cliente-DTP).

A parte executada no servidor (chamada de Servidor-FTP) é dividida em dois módulos com funções análogas aos seus equivalentes no cliente. Esses módulos são:

1. Servidor-PI
2. Servidor-DTP.

A conexão de controle, usada na transferência de comandos FTP e suas respostas, é realizada diretamente entre o Cliente-PI e o Servidor-PI, e a conexão de dados é estabelecida entre o Cliente-DTP e o Servidor-DTP.

4.5 Telnet

O aplicativo Telnet oferece o acesso de uma máquina remotamente. O Telnet dá a oportunidade de acessar sistemas e máquinas que estejam distante do nosso local atual. Para abrir um Acesso Remoto normalmente utilizamos telnet local.dominio porta onde local.dominio poderá estar em FQDN ou em IP e a porta normalmente é utilizado 23 como porta default.

A sessão remota inicia especificando em qual computador você deseja conectar-se.

A partir do momento que se inicia a sessão de trabalho remoto, qualquer coisa que é digitada é enviada diretamente para o computador remoto (note que você continua ainda no seu próprio computador, mas o programa telnet torna seu computador um terminal do outro computador).

Será solicitado um username e uma password para acessar o sistema remoto. Telnet oferece três serviços básicos:

1. define um terminal virtual de rede, que proporciona uma interface padrão para sistemas remotos; programas clientes não têm que compreender os detalhes de todos os possíveis sistemas remotos, eles são feitos para usar a interface padrão;
2. inclui um mecanismo que permite ao cliente e ao servidor negociarem opções e proporcionar um conjunto de opções padrão;

3. trata ambas as pontas da conexão simetricamente. Assim, ao invés de forçar o cliente para conectar-se a um terminal de usuário, Telnet permite um programa arbitrário tornar-se um cliente. Além disso, cada ponta pode negociar opções.

4.5.1 Funcionamento

Para logins remotos, há somente uma conexão, normalmente envia dados. Quando é necessário enviar comando (isto é, para setar o tipo de terminal ou trocar algum modo) um caractere especial é usado para indicar que o próximo caractere é um comando. O caminho dos dados em uma sessão remota é como uma viagem do terminal do usuário para o sistema operacional remoto

4.5.2 Usando Telnet

Para chamar o telnet:

```
A=í Éä å Éí ==
```

O programa telnet apresenta então o seu prompt (telnet>) ao usuário, para receber novos comandos. O telnet também tem o comando help.

```
í Éä å Éí [ =ÜÉä é =
```

Mostramos agora um exemplo de uso do comando telnet para listar o diretório de uma máquina remota. Desejando acessar informações que se encontram no computador chamado server.escola.edu.br, que está localizado fisicamente longe do computador do usuário, cujo o usuário seja joao e a password xxx.

```
A=í Éä å Éí =ë Éê î Éê KÉë Åç ä ~KÉÇì KÄê

ì ë Éê W=à ç ~ç

é ~ë ë ï ç ê ÇWñ ñ ñ

í Éä å Éí [ =
```

A conexão está estabelecida, portanto partir de agora tudo o que for digitado será executado na máquina remota.

```
í Éä å Éí [ =ä ë
```

Çê ï Çê ï J ê ï NMOQl Åí =NR=NOWMM=K
Çê ï Çê ï J ê ï NMOQl Åí =NR=NOWMMKK
J ê ï J ê J ê J NP QQQk ç î =OP =ONWRM=~ê è ì á î ç NKò á é
J ê ï J ê J ê J NTMT=k ç î =OP =ONWRR=~ê è ì á î ç OKò á é

Para encerrar a sessão de trabalho remota:
í Éä å Éí [=ä ç Öç ì í ==

O grande problema do Telnet é que ele não é criptografado, portanto, tudo o que é digitado no terminal (inclusive senha) pode ser lido por qualquer usuário ligado nesta rede. Para resolver isso pode-se usar o aplicativo SSH (Secure Shell), de funcionamento semelhante ao telnet, porém toda a comunicação é criptografada, além de várias funcionalidades de segurança.

Atividades de avaliação

1. Sobre o serviço DNS diga o que é um Serviço de Nomes, Domínio de Nomes e Resolução de Nomes.
2. Comente a importância do WWW para o difusão da Internet pelo mundo.
3. Quais os tipos de mensagem usadas no protocolo HTTP?
4. Quais os tipos de métodos utilizados no protocolo HTTP e quais suas principais características?
5. O que é uma URI? Dê um exemplo.
6. Quais são os componentes de uma transmissão de e-mail? Explique a função de cada um.
7. Explique o funcionamento do protocolo SMTP.
8. Comente as principais funcionalidades do protocolo FTP.
9. Quais são os componentes de uma transmissão FTP? Explique a função de cada um.
10. Se o FTP implementa um modo de transmissão binário, o arquivo é transmitido exatamente igual, para que serve o modo de transmissão ASCII que só permite caracteres alfanuméricos?
11. Comente as funcionalidades do protocolo Telnet. Quais são os pontos de fragilidade do protocolo Telnet? Como essas deficiências podem ser resolvidas?

Síntese do capítulo

Nesta unidade apresentamos os conceitos básicos dos protocolos Internet. Começamos com os conceitos de um protocolo de rede genérico e o protocolo IP, tanto na versão 4 como na versão 6. Em seguida apresentamos os conceitos de roteamento na Internet e os principais protocolos. Mostramos então os protocolos da camada de transporte, TCP e UDP. Finalmente, apresentamos algumas aplicações Internet como dns, e-mail, http, ftp e telnet.

Leituras, filmes e sites

Sites

Página da Wikipedia com vasto material sobre Protocolo Internet (em português)

http://pt.wikipedia.org/wiki/Protocolo_de_Internet

Internet Architecture Board (IAB) órgão normativo da Internet (em inglês)

http://www.iab.org/

Página do projeto Aprenda Internet Sozinho Agora (AISA) (em português)

http://www.aisa.com.br/index1.html

Referências

ANDREW S. TANENBAUM **Redes de Computadores** 4ª Ed. Editora: Campus, 2004. Livro de referência clássica com mais de 30 anos desde a primeira edição, proporcionando ao estudante uma visão histórica das arquitetura e protocolos de redes de computadores. São quase 1.000 páginas de texto com descrição detalhada dos sistemas e protocolos, além disso, o autor tem um ótimo senso de humor tornando a leitura muito agradável.

LARRY L. PETERSON & BRUCE S. DAVIE **Redes de Computadores: uma Abordagem de Sistemas.** 3ª Ed. Editora: Campus, 2004. Livro texto, tratando não apenas da descrição dos sistemas de redes de computadores mas fornecendo uma explicação do funcionamento. É um livro introdutório mas completo e coeso. Essa edição apresenta assuntos atuais como IPv6, redes peer-to-peer e redes móveis.

DOUGLAS E. COMER **Interligação em Rede com TCP/IP.** 5ª Ed. Editora: Campus, 2006. Livro texto completo sobre a arquitetura TCP/IP. Mostra os princípios de projeto da Internet, trata de endereçamento e roteamento IP, programação usando Sockets e exemplos de aplicações como e-mail e WWW. Mostra também assuntos avançados como IP móvel, VPN e MPLS.

KEITH W. ROSS & JAMES F. KUROSE. **Redes de Computadores e a Internet: Uma Abordagem Top-down.** 3ª Ed. Editora: Addison-Wesley, 2006. O grande diferencial desse livro, desde sua primeira edição, é a proposta inovadora da visão top-down no estudo dos conceitos de redes de computadores, isto é, começando na camada de aplicação e descendo até a camada física. Mas independentemente da visão adotada, é um excelente livro com conteúdo detalhado e leitura agradável. Quem preferir a visão tradicional, bottom-up, pode começar pelo último capítulo.

DOUGLAS E. COMER. **Redes de Computadores e Internet.** 4ª Ed. Editora: Bookman, 2007. Livro clássico sobre TCP/IP de fácil leitura e apropriado para leitor iniciante. O livro apresenta uma visão superficial mas completa de todos os protocolos da pilha TCP/IP.

Sobre os autores

Marcial Porto Fernandez nasceu no Rio de Janeiro em 1964, é Engenheiro Eletrônico pela UFRJ (1988), Mestrado (1998), Doutorado (2002) em Engenharia Elétrica, área de Teleinformática na COPPE/UFRJ e Pós-doutorado (2010) na Universidade Técnica de Berlin (TU-Berlin). Atualmente é pesquisador e professor adjunto do curso de Ciência da Computação na Universidade Estadual do Ceará (UECE) onde realiza pesquisas sobre redes de computadores, gerenciamento de redes, qualidade de serviço e redes móveis. Ele pode ser contactado através do e-mail marcial@larces.uece.br ou na página http://marcial.larces.uece.br/.